COVID-19 Apps

SOUTH AFRICA PROJECT REPORT

BY ALT ADVISORY

question convention
altadvisory.africa

TABLE OF CONTENTS

altadvisory.africa

LIST OF ACRONYMS

ACLED	Armed Conflict Location and Event Data Project
API	Application Programming Interface
CHW	Community Health Workers
CSIR	Council for Scientific and Industrial Research
ENS	Exposure Notification Server
HSRC	Human Sciences Research Council
ICT	Information and Communications Technology
NDOH	National Department of Health
SANDF	South African National Defence Force
SAPS	South African Police Services
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communication Act
R2K	Right2Know Campaign
USSD	Unstructured Supplementary Service Data
WHO	World Health Organization

INTRODUCTION

Country context

Country snapshot

South Africa is a vibrant and multi-cultural constitutional democracy with a painful past, unequal realities, and an uncertain future. With an estimated population of 58.78 million, it remains one of the most unequal societies in the world (World Bank, 2019). Covid-19 has in many ways highlighted – and exacerbated – the various divides in the country, which cross racial, socio-economic, gender, nationality and geographical lines (IMF, 2020). While South Africa has taken significant strides in advancing human rights and promoting equality and inclusion over the last 25 years, the painful legacy of apartheid persists, with discrimination and inequality reflected in the lived realities of many.

Despite ranking as the second-largest economy in Africa, South Africa is not economically stable (Bloomberg, 2020). Increasing government debt and low growth trends in 2020 indicate a negative economic outlook. Unemployment remains a significant concern with approximately 2.2 million jobs lost in the second quarter of 2020 (Fitch Ratings, 2020; Labour Force Survey, 2020). This makes many people dependent on the state for social grants and other forms of public benefit assistance. Covid-19 and the measures adopted by the South African government have had, as elsewhere in the world, a devastating effect on the economy. The immediate economic costs occasioned by the lockdown imposed in March 2020, the amplification of pre-existing economic challenges, and the longer-term repercussions of the pandemic are likely to continue to have profound economic implications (Arndt et al., 2020).

South Africa's economic stability is closely aligned with the country's political climate. In recent years the political landscape has been tainted by corruption scandals, an accountability crisis and failing state institutions. The African National Congress (ANC), which has been the ruling party since South Africa emerged as a constitutional democracy in 1994, obtained nearly 60% of the seats in Parliament following the 2019 national elections (PMG, 2019). This has led to concerns that South Africa is closer to a dominant-party system than a multiparty system (Himbara, 2020). A judicial commission of inquiry is presently underway to investigate allegations of state capture, corruption and fraud committed in the public sector and by organs of state. Regrettably, and amidst the current global crisis, corruption has remained rife with widespread allegations of irregular procurement procedures relating to personal protective equipment (Transparency International, 2020).

Protection of the right to privacy

Privacy and surveillance hold historical significance in South Africa, with the apartheid government relying on invasive and unscrupulous tactics to monitor and oppress large portions of the nation (McKinley, 2016). While the democratic government has committed internationally and domestically to protect and promote the right to privacy, unlawful interference with this right coupled with inadequate safeguards in the use of surveillance practices has seen, particularly in recent years, the erosion of the right to privacy (R2K and Privacy International, 2020).

Despite the historical and contemporary challenges, South Africa is in many ways a robust vibrant constitutional democracy, with an active civil society, an independent media, and an impartial judiciary. The Constitution of the Republic of South Africa, 1996 is the foundational legal framework and the supreme law of the country that is binding on both the state and the private sector, to the extent applicable. In terms of information rights, the Constitution guarantees the rights to freedom of expression and access to information and privacy.

Freedom of expression and access to information are detailed in sections 16 and 32 of the Constitution. The right to privacy is contained in section 14, which provides, in part, that "[e]veryone has the right to privacy". Under the terms of section 36 of the Constitution this may only be limited by a law of general application and to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.

The reality, however, is that these constitutional safeguards notwithstanding, privacy protections in the country remain inadequate. The Constitutional Court recently declared several provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) unconstitutional. RICA is the law that permits the interception of anyone's communications by authorized state officials, subject to prescribed conditions. The Court ultimately found that RICA is unconstitutional in five important respects because it did not provide sufficient safeguards to protect the privacy of citizens. It also confirmed that bulk surveillance is unlawful in South Africa (*AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* [2021] ZACC 3). This case was premised primarily on alleged violations of the right to privacy, after it was divulged that a prominent journalist had been placed under surveillance. Moreover, while the Protection of Personal Information Act 4 of 2013 (POPIA) was signed into law in 2013, the substantive provisions will only be enforceable from 1 July 2021.

Covid-19 in South Africa

To date, South Africa has had approximately 1,509,124 cases of Covid-19, with approximately 1,424,401 recoveries and 49,667 deaths (SA Coronavirus, 2021). In response to the pandemic, President Cyril Ramaphosa declared a national state of disaster according to the Disaster Management Act 57 of 2002 (DMA) in March 2020. This is distinct from a state of emergency and does not permit any derogation of rights. The state of disaster has been extended into 2021. The country went into lockdown from midnight on March 26, 2020, with a risk-adjusted strategy that is guided by, among other things, the level of infections and rate of transmission, the capacity of health facilities, the extent of the implementation of public health interventions, and the economic and social impact of continued restrictions (SA Coronavirus, 2020). South Africa has progressively moved to the less restrictive levels; however, following the second wave and a significant increase in numbers during the festive season, South Africa has returned to level 3 – with various restrictions on movement, economic activity and social gatherings.

Overview of the report

This research report employs a qualitative approach, comprising: (i) a literature review, including reports from previous studies, media reports, academic works, and government documents; (ii) a legal and policy analysis, including relevant legislative and policy developments; and (iii) key informant interviews with purposively selected respondents. We conducted 13 interviews with several privacy activists and public health activists, journalists and academics. We further engaged with officials from the National Department of Health, the private sector, and the judge designated to oversee the geolocation contact tracing process implemented by the South African government.

We gratefully acknowledge the efforts of those who generously shared their personal experiences, insights, and time. Their input assisted in informing our thinking and helped bring this report to life. We are thankful to the experts who gave their time and agreed to be interviewed. We are particularly grateful for the expert tips they provided. Thanks, in this regard, go to Anre von Delft (Doctor/Activist, TB Proof), Elri von Delft (Journalist, Spotlight), Gabriella Razzano (Consultant, Open Up), Gaurang Tanna (Head: Policy Co-ordination and Integrated Planning, National Department of Health), Maria Carpenter (Head of Digital Channels, Discovery), Nikhil Naik (Intermediate Business Analyst, Discovery), Ingrid Schoeman (Doctor/Activist, TB Proof), Jane Duncan (Academic, University of Johannesburg), Kungela Mzuku (Co-founder, Covi-ID), Catherine O'Regan (Designated Judge to oversee Covid-19 Tracing Database), Thami Nkosi (Activist, Right2Know Campaign), Debbie Rogers (Managing Director, Praekelt), Taryn Hinton (Consultant, Praekelt), Murray Hunter (Activist), and Sam Sole (Journalist, amaBhungane Centre for Investigative Journalism).

Throughout the research and the engagements with partner organizations working on this project, it became increasingly apparent that while South Africa's response to the pandemic has not been perfect, there are many facets of the responses that are commendable. We note that comparatively, South Africa has made significant strides in seeking to safeguard privacy and promote the protection of personal information. We do, however, acknowledge that there have been some shortfalls, and there is still a lot of work to do to ensure that responses are both effective and respect an array of fundamental rights.

The report seeks to assess the various responses of the South African government, both technical and non-technical. Our key findings can be summarized as follows. First, the "COVID Alert SA" app (South Africa's official contact tracing free exposure notification app) has had a limited impact from a public health perspective, raises some privacy and data protection concerns, and has not led to significant exclusion or discrimination of vulnerable populations. Second, "COVIDConnect" (the official government Covid-19 WhatsApp channel) has had some direct and indirect impacts on public health, it has several privacy concerns, and, like the COVID Alert SA app, does not appear to be particularly problematic from an equality perspective. Third, the alternative measures adopted by the South African government, such as the national lockdown, a contact tracing database, and prohibitions on disinformation, have had mixed impacts from a public health perspective, have caused some privacy and free speech concerns, and have led to significant challenges for vulnerable populations.

We hope that this research and the recommendations can support the South African government's continued response to the pandemic, and that by highlighting various successes and failures, we can map out a rights-based strategy for current and future responses to crises.

PILLAR 1: EFFICACY OF APP RESPONSES FROM A PUBLIC HEALTH PERSPECTIVE

Assessment of app response

COVID Alert SA

On September 1, 2020, South Africa's official contact tracing free exposure notification app, "COVID Alert SA", was launched (NDOH, COVID Alert SA). The app is built on the Apple-Google Exposure Notifications (GAEN) API and works via Bluetooth by sending exposure notifications to users if they have been in close contact with another app user who has tested positive for Covid-19. The NDOH explains:

> "When an app user anonymously reports to the app that they have COVID-19, the COVID Alert SA app sends notifications to those devices that were in close contact with this person's device. These exposure notifications warn those app users that they could potentially have been exposed to the virus. App users are guided as to what to do next to optimise their wellbeing and prevent the spread of the COVID-19 virus to others. At no stage does the app reveal the users' identities." (NDOH, 2020)

Before turning to details of how the app works, it is necessary to give a brief overview of the timeline of the app's development. In April 2020, Discovery Limited[1] – a leading private medical insurer in South Africa – began exploring ways in which technology could be used to combat Covid-19. At the same time, the NDOH were working on their technical response in the form of "COVIDConnect", which began as a WhatsApp channel to provide accurate information about Covid-19. COVIDConnect was developed in partnership with the NDOH, Telkom,[2] Praekelt,[3] GovChat,[4] and the Council for Scientific and Industrial Research (CSIR).[5] Over the next few months, COVIDConnect expanded to become a service that provides healthcare information, screening, and contact tracing processes.

The WhatsApp channel started in March 2020 and the self-assessment and risk-assessment screening services were available by April 2020. COVID Connect, as a contact tracing process, was piloted in June 2020 and launched nationally in July 2020. By July 2020 Discovery and the South African government – including the office of the Presidency and the NDOH – agreed to proceed with developing an app. COVID Alert SA launched

[1] Discovery services include medical aid, car insurance, banking, and life insurance. Discovery currently covers over 5.1 million clients. See https://www.discovery.co.za/portal/.

[2] Telkom is a leading ICT services provider in South Africa, offering fixed-line, mobile and data services and information technology services. See https://www.telkom.co.za/today/.

[3] Praekelt is an organization that designs technology-based programs, products, services, and experiences to support individuals and communities on a variety of issues. See https://www.praekelt.org/.

[4] GovChat is South Africa's largest civic engagement platform accessible online, on any mobile handset and feature phones. See https://www.govchat.org/.

[5] The CSIR is a leading scientific and technology research organization that researches, develops, localizes and diffuses technologies to accelerate socioeconomic prosperity in South Africa. It was established by an Act of Parliament in 1945. The CSIR's shareholder is the South African Parliament, held in proxy by the Minister of Science and Technology. See https://www.csir.co.za/.

in September 2020. As will be described in further detail below, the NDOH views COVIDConnect and COVID Alert SA as complementary services that sought to assist the fight against the virus.

Discovery developed the app software on behalf of the NDOH and continues to provide technical support services. The entire system for the app is under the direct control of the NDOH and is operated technically on its behalf, by the NDOH, Discovery, and Telkom. Telkom provides the CovidConnect service which validates test results to ensure fidelity of the system.

Understanding the COVID Alert SA app

We secured an interview with the NDOH and members of the Discovery team who worked on developing COVID Alert SA. We conducted two interviews, during which they provided detailed insights into the development and functioning of the app. The explanation below is based on these interviews, as well as publicly accessible information about the app (NDOH, COVID Alert SA).

- **Step 1** – **Download**: The app is available for download on the Google Play Store, Apple Appstore and Huawei App Gallery. Only certain operating systems are compatible with the app (android devices of 6 and above and iPhone devices of model 6s). The COVID Alert SA website indicates that the app has been developed to keep the download size under 3 MB; however, during the interview with the app developers, it was noted that while the first version was under 3MB to download, the current version is slightly bigger, requiring just under 10MB to download and just under 10MB to install. The app developers noted that this amount was insignificant for most people who have smartphones.

- **Step 2** – **Getting Started:** During the installation process there is a fairly detailed onboarding process. At this stage, the app provides users with information about receiving notifications, sending notifications, privacy protections, and next steps on how to manage your health if you have tested positive. There is further explanation about exposure notifications. At this stage, users can select if they want to "enable COVID-19 Exposure Logging and Notifications." Thereafter the app prompts users to allow or not allow notifications. The app then advises users on why it is important to alert others if they have tested positive – noting that this can help break the chain of transmission.

- **Step 3** – **Learn More**: This navigation contains information about the app, how it works, the privacy protections, information about location data not being collected or stored, and how random codes are used. The "learn more" navigation also provides information on the next steps in terms of possible exposure or positive diagnosis. It provides basic information about self-quarantine, self-isolation, and monitoring symptoms, and details of a 24-hour hotline as well as the WhatsApp information service number (WhatsApp chatbot).[6]

- **Step 4** – **Exposure Notifications:** The app developers took us through a demonstration of the exposure notification process, and explained it as follows:
    - Person A and person B come into close contact with one another. Close contact is approximately two meters for a period of 15 minutes, as per the WHO guidelines. Both person A and person B need to have the app and need to have their Bluetooth on. During the 15 minutes of close

[6] The app developers explained that when using the WhatsApp chatbot privacy is not maintained because the user is choosing to use their WhatsApp application. This will be discussed in more detail under Pillar 2.

contact, each device is generating randomized codes. Following the Bluetooth connection, person A's codes are swopped with person B. Each person retains their code as well as the new code from the other person. The codes are then stored on the device.

- A few days later person A starts feeling ill and decides to go for a Covid-19 test. Person A's test results are positive. The results are communicated via SMS from the NDOH and include a unique PIN code.
- Person A decides to alert others using the COVID Alert SA app. The person inputs their unique PIN into the app under the "Alert Others" navigation. At this stage, the app requests the user to input their date of birth. The app developers explained that this unique PIN is sent to a cell phone number to ensure accuracy as handwritten numbers relied on at testing stations may lead to typos or the unique PIN being sent to the incorrect person.
- Once the date of birth is provided, the app asks if you want to share your device's random IDs with the app. If person A chooses to share their diagnosis, an exposure notification is sent to others who they have been in close contact with.
- Person B then receives a notification of possible exposure. The app explains that you were exposed to a person with a positive diagnosis on a particular date. The app does not provide time of day or location in relation to the possible exposure. The app developers explained that location data are neither collected nor stored and that while they could have included the time of the possible exposure, they felt it was not necessary for people to try to ascertain who or where the possible exposure was from.

The terms and conditions also detail important information about the app and how the app works**.** In this regard, users are anonymously informed via the app if they have been in close proximity with a user who has tested positive for Covid-19. Once enabled, a user's device will regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier code (a string of random numbers that are not tied to a user's identity, and that changes every 10-20 minutes). As mentioned, the app uses the GAEN frameworks to allow Bluetooth to estimate the distance from other phones running the app, while other phones are monitoring for these beacons and broadcasting theirs as well. When each phone receives another beacon, it will record and store that beacon on the device, including the signal strength, date and estimated duration of proximity. At least once a day, the system will download a list of the keys for the beacons that have been verified as belonging to people confirmed as positive for Covid-19. Each device will check the list of beacons it has recorded against the list downloaded from the server, and if there is a match between the beacons stored on the device and the positive diagnosis list, the user will be notified and advised on the next steps to take. A match is determined based on a risk-scoring algorithm, which considers the random codes from the device of the user who tested positive for Covid-19 to assess whether the proximity or duration of the contact between the two users is considered to be of significant risk to warrant the interaction being stored. According to the terms and conditions, the NDOH may revise the risk-scoring algorithm from time to time in consultation with other experts.

The terms and conditions state further that if you test positive for Covid-19, the NDOH generates a unique PIN and sends it to you via SMS. If you are a user of the app, you can voluntarily share your random IDs with the app by entering this PIN into the app. The NDOH uses this unique PIN combined with the user's date of birth to ensure a valid positive diagnosis and upload keys. According to the terms and conditions: "Without ever sharing who you are, this allows us to alert other app users that they are at risk of exposure to COVID-19 because someone they have spent time near has tested positive for COVID-19." As will be dealt with in more detail below, the app collects a temporary exposure key for all users. For users who test positive and

elect to alert others, the app collects their Covid-19 positive test status, their unique PIN supplied with their test results, and their date of birth. If a user loses their PIN, and chooses to follow the lost PIN journey, then the app will collect their name, surname, date of birth, and cell phone number.

Reflections on the effectiveness of the app from a public health perspective

There are no clear data at this stage that capture the efficacy of the app from a public health perspective; however, there are certain indicators that can be relied on when reflecting on the effectiveness. To this end, we have considered the effectiveness of the app using three indicators: (i) uptake (number of people using the app); (ii) user experiences; and (iii) public perceptions of the app. Before turning to these indicators, it is worth noting that one of the public health experts we interviewed felt that the app was good from a public healthcare perspective, noting that it will likely add a lot of value. He did, however, note that uptake may be an issue for two reasons. The first is the current general distrust of the government. Here he noted concerns around corruption, poor service delivery, surveillance, and privacy. Second, he highlighted issues around the digital divide in South Africa. He suggested that these issues may impact the efficacy of the app from a public health perspective. Judge O'Regan – the judge appointed to oversee the initial efforts of contact tracing in South Africa – noted that the app is not an effective way of managing the Covid-19 pandemic because of low uptake and low levels of trust. Judge O'Regan also observed that in comparison to government messaging around the risk-adjusted strategy and the various levels of lockdown – which for the most part were well understood by people in South Africa – she felt that there was not the same level of understanding of the app, its purpose, and how it worked. It is therefore likely that, alongside trust issues, a lack of focused and targeted communications and general understanding of how the app works may have also contributed to its limited impact from a public health perspective. While issues around privacy and the digital divide will be addressed further under Pillar 3, it is important to note that these concerns feed into the assessment of the efficacy of the app from a public health perspective.

For the app to be effective, enough people will have to download it. Three weeks after it was launched, reports announced that over 500 thousand people had downloaded the app (Business Insider, 2020). At the time of our interview with the NDOH in October 2020, there had been 650 thousand downloads. By December 3, 2020, as South Africa was approaching its second wave, approximately a million people in South Africa had downloaded the app (Ramaphosa, 2020). As of February 2021, Google Play records 1 million+ installs. The Huawei App Gallery has recorded 236 thousand downloads. The number of downloads from the App Store does not appear to be readily available. The NDOH are hoping for five million downloads. While there is some debate regarding how many people need to download a contact tracing app for it to be effective, it appears that in the South African context, a generous estimate of a download rate of 7% of the population[7] makes it unlikely that the app has made significant inroads in curbing Covid-19 (O'Neil, 2020, Bhana, 2020). The South African government, including the NDOH, along with several private sector actors, are working on encouraging people to download the app.[8] The NDOH states that:

[7] This is a rough calculation based on an understanding that there are approximately 28 million smartphone device subscribers in South Africa. See Independent Communications Authority of South Africa, The State of the ICT Sector Report in South Africa (2020) at 34 (accessible at https://www.icasa.org.za/uploads/files/State-of-the-ICT-Sector-Report-March-2020.pdf). Estimating that two million people have downloaded the app, it appears that roughly 7.1% of the smartphone-using population have downloaded it.

[8] Several banks and mobile network operators have incorporated referral programmes on their apps to encourage users to download COVID Alert SA.

> "By downloading and using the COVID Alert SA app, you become a part of a powerful digital network of app users who choose to work together for the benefit of everyone in the app community while all enjoying complete privacy and anonymity. App users understand their exposure to COVID-19 and help others to do the same. We can all work together to curb the spread of COVID-19 and, ultimately, to save lives." (NDOH, 2020)

Public mistrust of the government appears to have contributed to the public's response to the app. Several of our interviewees noted that people's scepticism from a privacy perspective was not misplaced given the lack of an effective data protection framework, previous attempts by the government to track and monitor people, and a more general distrust of technology. Other interviewees noted that pervasive digital divides were a more likely reason for slow uptake. One public health activist noted that community members in informal settlements either do not have access to phones, and if they do, they are wary of telling officials that they have phones, and in any event, they often struggle with a signal too weak to download or use apps.

Related to the relatively slow uptake, we observed mixed reviews about the app on Google Play, the App Store and the App Gallery. While we accept that reviews on various app stores do not necessarily amount to sound empirical evidence, the reviews do provide some insight into user experience.[9] In January 2021, one iPhone user noted that of the six notifications of exposure, four had occurred on days where the only place she went to was a store for less than 15 minutes, with the latest exposure notification linked to a day when she did not leave her house. Another android user stated that she and her husband have the app, both tested positive and updated their status but neither had received exposure notifications.

Apart from concerns of this nature, it appears that users' frustrations are linked to a limited understanding of how the app works. One user noted "this App is a waste as it sends you notifications 5 days after you have been exposed to the virus. The App is supposed to tell immediately that you are near someone positive in order to move away from that location. It doesn't even tell you the location of where u was exposed. Really doesn't help because now I am COVID-19 positive when really this app should have told me immediately when I was initially exposed."

A media report from January 2021 similarly suggest that some users have complained that the app is not working effectively (Sonjica, 2021). According to the report the app developers have not received complaints about people getting notifications about being exposed to Covid-19 when they had not been out during the purported exposure period. The report further notes that the app developers and the NDOH are concerned that those who are dissatisfied with the app may not understand how the app works. Accordingly, users have been encouraged to gain a better understanding of the app. (Sonjica, 2021). While the above responses do not necessarily reflect the views of all users, it appears that, through our informal engagements with app users as well as recent media reports, there are degrees of frustration and dissatisfaction with the app, which indicate that people may not perceive the app as effective from a public health perspective.

During our interviews, particularly with digital rights experts, issues were raised around the timing of the launch of the app as well as perceived political motivations. In an interview in early November 2021, it was suggested that the launch was more of a political act – a box ticking exercise – to show that South Africa was engaging in tech-based responses. The interviewee explained that there was limited and inconsistent

[9] We equally accept that only 2,735 reviews have been posted across the three app stores. Therefore, the views expressed in the reviews may or may not reflect the views of the majority of users.

marketing around the app – apart from Discovery – generally targeting a middle to upper-class audience. The interviewee took the view that the government did not believe that the app is an effective part of its strategy. Unsurprisingly, a different perspective was provided in the interview with the NDOH. The NDOH explained that the app is meant to be a health promotion tool – a fourth prevention measure along with hand hygiene, social distancing, and the wearing of masks. In subsequent media interviews, the NDOH described the app as being a potentially powerful public health tool, stating that "[y]ou have to try and put in place every additional modality that you can. Every 100 infections we avert with this technology we save two lives. And those two lives do matter. It's a fairly low-cost intervention and it's the least South Africans can do to help us fight Covid-19" (Nortier, 2020). Another goal of the app is to assist with other health challenges in the country such as TB or HIV.

While there may be validity in the argument that the inclusion of a tech-based response was a box ticking exercise, it is more likely that the app was included to be part of the solution – not *the* solution. The app has not been and may never become the most effective measure in addressing Covid-19. Its impact appears to be fairly limited at this stage. However, and notwithstanding concerns that will be addressed below, we conclude that its role in meaningfully responding to Covid-19 has been limited.

Additional app responses

Covi-ID

A team of students, scientists, and entrepreneurs from the University of Cape Town sought to develop a free, privacy-preserving app that provides an integrated track and trace solution. "Covi-ID" is set to be a health credentials solution specifically tailored for the African market. In an interview with one of the Covi-ID developers, it became apparent that their team intended to develop an alternative solution that was inclusive and responsive to the current realities of South Africa, noting that not everyone has access to a smartphone, or there are several members of a family using one phone. According to one of the developers, some data are needed to access and download the QR code, but the app is free to users.

A Covi-ID user's journey is as follows: A user will create a Covi-ID through the web application. The Covi-ID application programming interface (API) will generate a wallet for the user's specific account when the user creates their Covi-ID. When a person tests positive for Covid-19, they can choose to submit their test result and geolocation data to contact tracers. The data can then be used by manual contact tracers to identify other Covi-ID users who may have been in the same location as the infected person. The user is presented with a QR code that can be downloaded and stored either digitally or physically. This is a notable feature of Covi-ID. The ability to print out the QR code allows people who do not have access or consistent access to a smartphone to indirectly use the app. When entering public places with verifiers (such as security guards), users can present their QR code for scanning. The scan will reflect the user's Covid-19 status as green, red or amber. Subsequently, the user will either be granted or denied entry by the verifier, depending on the user's Covid-19 status. Covi-ID differs substantially from COVID Alert SA. While both apps pride themselves on their use of privacy-protecting technology, Covi-ID focuses more on verification and health status than contact tracing, despite having some manual contact tracing objectives.

Covi-ID's privacy policy notes that the app may collect, use, store, and transfer the following personal data: Identity Data including first name, last name, country of residence, username or similar identifier, date of birth

and gender; Contact Data including email address, physical address and telephone numbers; Medical Data including Covid-19 status as provided by an authorized medical practitioner; Biometric Data including age, gender, and photographs; Profile Data including application username and password, preferences, feedback, ratings and reviews, and survey responses; Usage Data including information about app use , application, surveys and services; and Marketing and Communications Data including preferences for receiving notices and marketing from Covi-ID and their third parties as well as communication preferences. They also collect, use and share Aggregated Data such as statistical or demographic data. The privacy policy notes that personal data may be shared outside South Africa, but that protections and safeguards are in place.

It was noted during our interview that the app had not been formally rolled out, but it had been piloted in a local bank and a local market. The interviewee noted that the Covi-ID team has partnered with the Massachusetts Institute of Technology (MIT)'s PathCheck to increase access to the app. The intention, in time, is for MIT to approach governments with Covi-ID as an alternative, where they offer the Apple-Google solution, but also offer Covi-ID in areas where there is a low smartphone penetration rate. While the developers were initially in talks with the NDOH, the app was not ultimately rolled out by the government. It is therefore difficult to gauge its effectiveness from a public health perspective, but it does provide a useful alternative to consider in conjunction with other responses.

Healthcheck

Healthcheck is a web-based service that uses Unstructured Supplementary Service Data (USSD) and WhatsApp. It has been implemented by the Department of Higher Education and Training, together with HigherHealth and Praekelt. It is mandatory for all students and staff entering higher education facilities (University of Pretoria, 2020). While the primary purpose appears to be assisting with screening, it is also relevant to contact tracing as the information collected is added to the contact tracing database. Users are required to answer a set of questions on the platform to determine if they are low, moderate, or high risk. If the risk is low, the individual will receive clearance valid for 24 hours (SA News, 2020). Similarly to Covi-ID, the primary focus of Healthcheck is verification. Contact tracing appears to be a secondary consideration.

In a speech on September 30, 2020, the Minister of Higher Education, Science and Innovation stated:

> "The Higher Health daily Healthcheck and the issue of daily 'health passport' to every student, staff and stakeholder entering our campuses has assisted our sector with the identification of moderate to high-risk individuals and their referral for appropriate follow-up care. To date, over 5 million Healthcheck screenings have been administered since the launch of Healthcheck." (Nzimande, 2020)

Over 1.6 million students and staff across the sector are using Healthcheck on a routine basis, before entering the campuses. Apart from these numbers, there is little available evidence to determine the impact of Healthcheck from a public health perspective. Indeed, this has garnered little attention or scrutiny, even though it entails the collection of significant amounts of personal information daily, including personal details and any symptoms that the person may be experiencing. As a mandatory measure for persons wanting to access higher education facilities, this gives rise to serious concerns about privacy rights.

Assessment of alternative means

Risk-adjusted strategy and lockdown

In response to the Covid-19 pandemic, the primary measure instituted by the government was to declare a national state of disaster on March 15, 2020, which authorized the drafting and issuing of regulations and directions for the purposes of, among other things, protecting the public, providing relief, combatting disruption and dealing with the destructive and other effects of the disaster. On March 23, 2020, the President announced a 21-day lockdown with effect from midnight on March 26, 2020. People in South Africa were required to stay at home and were only allowed to leave their homes under strictly controlled circumstances, such as to seek medical care, buy supplies, or collect a social grant.

On May 1, 2020, the South African government implemented a risk-adjusted strategy, with level 5 being the highest risk and level 1 the lowest. For example, under level 5 drastic measures were imposed to contain the spread of the virus. This included all South Africans having to stay at home, unless performing an essential service, obtaining an essential good or service, collecting a social grant, or seeking emergency or life-saving medical attention or care for chronic medical conditions (Ramaphosa, 2020). Extreme precautions were introduced under level 4, allowing some economic activity to resume. There are some restrictions on activities at work and social settings under level 3. Level 2 requires physical distancing and some restrictions on social activities, and at level 1 most normal activity is expected to resume. In December 2020, following the emergence of a second wave of Covid-19 in the country, President Ramaphosa announced that South Africa would move from level 1 to level 3, with additional restrictive measures being implemented over the end-of-year festive period, including a curfew and a ban on the sale of alcohol. At the end of February 2021, South Africa moved back from level 3 to level 1.

Reactions to Covid-19 responses have ebbed and flowed. The March 2020 lockdown was initially hailed by many as exemplary, but by June 2020, South Africa was ranked in the ten most affected countries in the world for its Covid-19 numbers, with many critical of the response, raising concerns that the social and economic implications could be catastrophic (Naude and Cameron, 2020). It is necessary to note that "compliance with lockdown orders presented a greater challenge among rural populations and others with more precarious livelihoods", thereby deepening pre-existing divides (Carlitz and Makhuru, 2021).

Manual contact tracing

According to a report in the Financial Times, approximately 280 thousand health workers were mobilized in April 2020 to screen over seven million people – approximately one in ten South Africans (Medical Brief, 2020). This approach draws heavily on South Africa's experience with managing HIV and TB, and many of the structures for such contact tracing were already in place. We interviewed healthcare professionals from TB Proof (a South African NGO committed to TB prevention, stigma reduction, and access to quality TB treatment), who enthusiastically promoted the role of manual contact tracing. TB Proof relies heavily on community health workers (CHW) to build trust in communities and establish relationships with community members. CHW further assist in reaching people with TB who are not accessing health services and linking them to healthcare. Household contact tracing of newly diagnosed TB patients has been found to be an important component of comprehensive strategies to end TB in rural high-burden settings (Little et al., 2018).

As stated in the Financial Times report, "Whereas other countries need to hire thousands of people to conduct screening and contact tracing – the US would require at least 100,000 contact tracers at a cost of $3.6 billion, according to one estimate – South Africa already had teams in place, detecting tuberculosis, a national killer, and bringing drugs to the millions of South Africans living with HIV" (Medical Brief, 2020). The Human Sciences Research Council (HSRC) found that efforts to fight the TB epidemic in South Africa provide valuable lessons that can assist the response to Covid-19, including working with CHW who use a well-established system of contact tracing (HSRC, 2020).

The reliance on manual contact tracers appears to have been relatively effective. According to the same report, approximately 3% of the tests referred from CHW came back positive, similar to the proportion of positive results among patients tested at health centers, which suggests that the CHW were able to successfully identify the cases that might have otherwise slipped through the net (Medical Brief, 2020).

In practice, the process of manual contact tracing required the healthcare worker to interview an infected person to establish who they may have been in contact with (specifically, close contacts with whom they have had face-to-face contact of more than 15 minutes, or those with whom they have shared an enclosed space for more than two hours) (News24, 2020). The Red Cross in South Africa, in an interview regarding contact tracing methods, explained that: "There are different ways of reaching out, but most people are simply contacted by phone. There is no specialised technology that we use. Contact tracers make use of radio stations to reach people who may have attended gatherings, but in most cases, it takes a phone call or text message. The process of tracking must, however, incorporate personal distancing to reduce infection. We call people and send messages via SMS or WhatsApp and follow those messages up with a phone call" (News24, 2020).

While this is an effective measure, there have also been several challenges. Firstly, there have been wide variations in the approach and number of tests administered in each of the nine provinces. The process is also time-consuming and resource-intensive. The outcomes are dependent on whether the person interviewed can remember the names and contact details of all persons they have been in contact with. Furthermore, asymptomatic cases cannot be identified. One interviewee also advised that, although this approach was intended to be coupled with digital technologies, including apps to relay the test results more efficiently, a lack of training and availability of devices meant that there was an inconsistent application of these technologies.

Contact tracing database

On March 26, 2020, the Minister of Communications and Digital Technologies issued directions in terms of the Disaster Management Act (Directions, 2020) that provided for authorities to access location-based data. This appeared to contemplate increased surveillance powers by the state (Singh and Power, 2020). When interviewed, Professor Jane Duncan noted that the directions were very thin on details but seemed to suggest that their approach to contact tracing would be quite invasive, with no indications that there would be privacy protection. This provision of the directions has since been revoked.

In April 2020, Amended Regulations were published in terms of the Disaster Management Act. These explicitly provided for contact tracing (Amended Regulations, 2020). According to Professor Duncan, these regulations were a huge step up. Regulation 11H provided, among other things, for the establishment of a Covid-19 Tracing Database to enable people who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted Covid-19 to be traced. According to the Regulations, the

Covid-19 Tracing Database shall include all information considered necessary for the contact tracing process to be effective, including but not limited to: (a) the first name and surname, identity or passport numbers, residential address and other address where the person could be located, and cellular phone numbers of all persons who have been tested for Covid-19; (b) the Covid-19 test results of all such persons; and (c) the details of the known or suspected contacts of any person who tested positive for Covid-19. The Amended Regulations stipulated that information contained in the Covid-19 Tracing Database and any information obtained through this regulation is confidential. No-one may disclose any information contained in the database or any information obtained through this regulation unless authorized to do so and unless the disclosure is necessary for the purpose of addressing, preventing or combatting the spread of Covid-19. The amended regulations contain further safeguards to protect privacy rights, including user notification and the express provision that the interception of the content of communications is not permitted. Additionally, the appointment of a credible designated judge to oversee the process is considered an important step for ensuring that, to the extent possible, people's privacy and personal information are safeguarded.

We were fortunate to have the opportunity to engage with Judge O'Regan, the designated judge, and found her insights of great use. She explained that her role was very narrow and clearly defined in the regulations. When she accepted the role, she expressed very clearly that she would not provide her views on whether the Amended Regulations passed constitutional muster, advising that a different institution would be better placed to do so.

She noted that her role had three elements: (i) to receive weekly reports of the people whose location data had been provided by mobile network operators; (ii) to provide recommendations to the government about the content of the regulations and their application, balancing privacy rights and effective contact tracing methods; and (iii) to provide a post-state of disaster report. The regulations stopped short of giving her final authorization in these decisions around contact tracing, but she was empowered to make recommendations to ministers on amending the regulations (Hunter, 2020). She highlighted that the most important aspect of these roles from a policy perspective was the recommendatory role. In fulfilling her role, she did receive reports, but she noted that this took some time as she insisted that the sharing of this information must be done in a privacy-preserving manner. During the weeks of April 24, May 1, May 8, and May 15, 2020, Judge O'Regan received what she estimates were the names and mobile numbers of over five thousand people whose details had been requested.

During this period Judge O'Regan held meetings with the NDOH where she noted right from the start that she thought it was problematic that at a minimum the government needed to show that getting this location data would be an effective means of contact tracing. In her view, it was clearly not effective, leading her to provide recommendations to the NDOH as she considered that the original objective of the contact tracing regulations was unfeasible. Her other recommendations included: (i) government should not persist with contact tracing through mobile network data; (ii) that it should explore the use of aggregated network data for "hotspot" mapping; (iii) that it should explore the deployment of contact tracing apps in other countries to assess what would be feasible and appropriate in South Africa; and (iv) government should undertake independent security audits of the systems it had set up (Hunter, 2020). Shortly thereafter, the government elected to no longer request location-based data and shifted to the CovidConnect and COVID Alert SA tools.

Based on our interaction with Judge O'Regan and other interviewees, it appears that the initial approach to contact tracing was largely ineffective from a public health perspective. Abandoning the requests for location-based data at such an early stage further illustrates its ineffectiveness.

Assessment of combined alternative means and app responses

COVIDConnect

As mentioned above, COVIDConnect was launched by the NDOH in July 2020 as the South African government's official Covid-19 support service. COVIDConnect provides a useful example of a combined alternative means and app response. Like COVID Alert SA, it illustrates the efforts of the South African government to work with the private sector to facilitate different responses to the pandemic. The NDOH is working with a range of private sector providers, including GovChat, Telkom BCX and the Praekelt Foundation (Hunter, 2020).

There are two core tenets to COVIDConnect. The first relates to access to healthcare information. Individuals who use COVIDConnect can easily access Covid-19 news and information, prevention tips and wellness advice. There is also a simple risk-assessment tool that will screen users for Covid-19 symptoms and give them advice on whether they should self-isolate or seek professional clinical assistance (Mkhize, 2020).

The second component relates to contact tracing. The platform uses a combination of WhatsApp and SMS interaction to invite users who receive a positive Covid-19 diagnosis to notify nominated contacts (Hunter, 2020). During our interview, the NDOH took us through how this aspect of COVIDConnect works. After a person is tested, they receive notification that their results are ready – in the form of an SMS. The SMS directs the person to a WhatsApp link. Once in the WhatsApp channel, the person is required to fill in their date of birth and upon successful validation of the mobile number and date of birth, they receive their test results. The platform has since been strengthened, and the unique PIN for the COVID Alert SA app can also be used on COVIDConnect. If a person tests positive a series of health status questions are sent to them. The WhatsApp chatbot then asks the person to share the contact details of people they have been in close contact with. The contacts are alerted that they may have been exposed to Covid-19 without disclosing who tested positive, which ensures privacy, and prompts them on the next steps to take (Razzano, 2020). In addition, the system can geo-locate the nearest quarantine and isolation facility for the user, as well as the nearest healthcare facility for patients or their contacts who are experiencing symptoms requiring medical attention. The NDOH explained that this worked well for known contacts, but is limited in terms of notifying unknown contacts, a limitation set to be addressed by COVID Alert SA.

It appears that COVIDConnect has had some impact from a public health perspective. Between June 28 and July 15, 2020, COVIDConnect dispatched 674,380 SMSs to users nationwide and relayed 326,522 test results (Mkhize, 2020). According to Praekelt, within the first seven weeks of the launch of the app, 6.2 million unique users had used CovidConnect, with 211 million messages processed, and an average of 750 thousand daily users (Praekelt, 2020). At the time of our interview with the NDOH on October 30, 2020, it was estimated that an average of one in four cases engaged this service. The NDOH has explained that South Africa was the first country in the world to build a WhatsApp channel like this for Covid-19: "The service was so well utilised that the World Health Organization borrowed it for global use" (Nortier, 2020 quoting Tanna of the NDOH). Despite the widespread uptake, the platform has its limitations. It did not reach everyone – between 30% and 40% of people in South Africa do not use WhatsApp. Unlike COVID Alert SA, the contact tracing component is limited

to known contacts, but there are limitations to this as well – not everyone knows or remembers who they have been in contact with. It is necessary to note that, like with COVID Alert SA, the intention of this platform was to contribute to and complement the NDOH's broader response to reducing the spread of Covid-19. The NDOH explained: "[o]ur intention was never to get to everybody [through COVIDConnect] but certainly to get to as many as possible so that the burden on our healthcare workers is managed. Certainly, when we had 14,000 cases a day that was a blessing" (Nortier, 2020 quoting Tanna of the NDOH).

The NDOH further hope that the technology used in COVID Alert SA and COVIDConnect can help with communication efforts with TB or HIV patients, in a secure and direct manner. It is worth noting that the TB Health Check App was launched on February 5, 2021. This app provides an easy way for people to screen themselves for TB. It guides users through a series of questions and then advises if they need a TB test or not. According to reports, over nine thousand South Africans have screened themselves for TB using the app, and over 600 people have received a TB test. Those who have tested positive are now receiving treatment (Msomi, 2021). This is a notable public health outcome of these technology-based responses.

PILLAR 2: CONTACT TRACING APPS AND FUNCTION CREEP – INCREASED SOCIAL CONTROL

Assessment of app response

COVID Alert SA

Data collected by the app

We were advised during the interview with the app developers that the user does not provide any personal information when downloading and installing the app; however, if they are diagnosed with Covid-19 then they can choose to alert others, which requires inputting their date of birth. According to the terms and conditions, the app is not capable of using the user's GPS to track their location; to enable law enforcement to identify or track the user; to access personal information or data saved on the phone; or to discover name, address or health information. The app records information in an encrypted, anonymous and de-identified form, depending on how close your device is to another app user; and the date and time of these events. The data is kept on your phone for 14 days, and anonymized data are uploaded and only used when notifying your positive status.

The app's privacy policy is designed to ensure that the app user is not identifiable and remains anonymous. No personal information is stored; only temporary exposure keys are stored on the central database. However, if a user chooses to upload their Covid-19 positive status, their unique PIN and date of birth will be stored. The Exposure Notification Server (ENS) stores random codes or "private key", and the date of private keys that it has collected over a period of 14-days. The ENS then send the random to all of the other app users. Each app user's device compares the random codes to check for a match of the codes that have been stored over the 14-day period. If there is a match the user is notified that they have potentially been exposed to Covid-19. During this process the identity of the users will not be shared with other users. In relation to data transfer, the ENS data list is made available to the app (or front end) in the retrieval process. The app uses an interface to the operating system of the user's mobile phone, which entails the processing of data by Apple or Google. The privacy policy notes that the operating system functions used via the interface complies with South Africa's data protection legislation – POPIA. All of these policies align with the findings of the technical review.[10]

[10] The technical review was conducted by independent technical experts in the context of this project. We have reviewed their findings and engaged with the technical reviewers on two occasions. See "Report on the privacy risks of COVID-19 software" (2020).

Privacy considerations

COVID Alert SA has been lauded by some for its privacy considerations, and the NDOH prides itself on the fact that "confidentiality and anonymity are core to the app's contact tracing process." The privacy policy explains that the purpose of the app is to provide strong protection for each user's right to privacy as provided for in section 14(d) of the Constitution.

The privacy policy provides that only state entities are allowed to control the app and that the system is only permitted to be used for contact tracing and by public health authorities. It further states that it does not share the identities of other users with Google or Apple. People who test positive for Covid-19 are not identified by the system to other users, to Google or Apple, or the NDOH, Discovery Limited or Telkom SOC Limited. Additionally, it provides that:

> "To protect data against unauthorised access, loss, or misuse the app makes use of a variety of sophisticated technical security measures (including, for instance, encryption; pseudonymisation, logging, access controls and restrictions). The NDOH and its partners also employ organisational strategies (including, for example, staff directives, confidentiality agreements, reasonably regular inspections) to ensure that all legal requirements have been, and are being, complied with."

The privacy policy stipulates that the app is based on the principle of "privacy by design." To this end, it states that: "through innovative encryption and cryptographic methods as well as decentralised data processing…as far as possible, no information relating to or identifiable persons (personal data) is present and that the risk of any possible re-identification is extremely low." In our research, we did not see any formal impact assessments but were advised by the NDOH and Discovery Limited representatives, that a few privacy experts had reviewed the app and had found it was sufficient from a privacy-preserving perspective. They indicated that the app had also been subject to scrutiny prior to launch by Judge O'Regan. They noted further that three penetration tests were conducted on the app by three separate groups of testers, including a private sector actor working pro bono, Discovery's internal information security team, and a team from the CSIR. The app developers noted that these tests confirmed that the app does what it says it does.
In our interview with Judge O'Regan she explained that while the app was presented to her by the NDOH, the app fell outside of her official remit. However, she did note that in her view the app was not problematic from a privacy perspective. Praekelt noted that COVID Alert SA is the gold standard both in terms of tech and in terms of privacy and data protection.

It is worth noting that South Africa's data privacy law, POPIA, will only be enforceable from July 1, 2021, therefore there was no strict legal requirement for a data protection impact assessment for the app. Notably, and as discussed in more detail below, the Information Regulator[11] encouraged voluntary compliance with the provisions of POPIA in the management and containment of Covid-19.

[11] The Information Regulator is an independent body established under POPIA. Among other things, it is empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA. See https://www.justice.gov.za/inforeg/.

Reflections on privacy concerns

Despite apparent safeguards, skepticism and scrutiny are not untoward. During our interview with a privacy activist, Thami Nkosi, he noted that there are pre-existing concerns regarding the state's previous conduct in relation to privacy. He explained that "the government has always had an appetite to have a peep into its society's happenings." Razzano has also been skeptical, noting that the role of Discovery Health in the COVID Alert SA app is no coincidence given that it is one of South Africa's most data-centric, big tech players. She cautions that "the stage for digital sovereignty in South Africa is being set, with only big tech and the state as the envisioned future actors" (Razzano, 2020). Further, the source code for the app is yet to be published. This too may contribute to feelings of distrust and the sense of a lack of transparency from the state and private sector.

It is necessary to highlight the concerns raised in the technical review of the app. First, the app's source code has been obfuscated and has not been made publicly available, which has frustrated efforts to understand the scope of processing activities undertaken by the app. The technical impediment complicates the analysis of the app by technical reviewers and goes against transparency criteria. The practice of releasing source codes, commonly known as "open source", has developed to allow the cybersecurity and technical community to inform developers about issues and even vulnerabilities present on their software.

Secondly, the technical reviewers detected a suspicious reference to a URL that potentially sends date of birth, cell number, name and surname to the backend servers. The technical reviewers were concerned that if confirmed, this would be contrary to the privacy claims reflected in Google Play's app description. In our interview with the app developers, we learned that the most recent version of the app – as of the interview on October 30, 2020 – includes a new functionality referred to as the "lost PIN journey". If you have not received or have misplaced your PIN you have a way of retrieving it. The app will ask for a user's first name, surname, mobile number and date of birth (information required when getting a Covid-19 test). This is to ensure that the correct PIN goes to the correct person, as in South Africa more than one person may share one device within a family or home. There is also the option of retrieving the unique PIN via WhatsApp. Following a further discussion with the technical reviewers, this may explain the unusual URL. However, the lost PIN journey and the data it requires do not appear to align with the app's privacy policy, which does not refer to the collection of a person's name, surname, or mobile number. The terms and conditions state that "your privacy is protected. The app is not capable of discovering your name or address, or your health information." Both the privacy policy and the terms and conditions should be updated to reflect the updates to the app.

Arguably the most concerning aspect for the technical reviewers is the reliance on WhatsApp as a communications platform. The technical reviewers explain that the use of WhatsApp's API to notify app users of the results of their Covid-19 tests raises privacy concerns, regardless of how convenient this may be. This approach might unnecessarily allow a third party with commercial interests to identify which users have been diagnosed as Covid-19 positive. This is not required by the GAEN framework and therefore appears to have been a choice made by the developers. Although the content of the messages is encrypted, one can anticipate that assumptions – such as a person's Covid-19 status - may be drawn when a user of the app engages the NDOH via the WhatsApp line.

Ultimately, while the government has established frameworks for heightened data protection and appears to be cognizant of privacy rights, it is wise to remain vigilant to the continued use of technical responses to both in the context of Covid-19 and beyond. We note the update to the app requires the collection of personal

information and are concerned that this has not been incorporated into the terms and conditions of the privacy policy. This poses concerns that future updates may similarly require personal data, and users would not find reference to this in the relevant policies. This is contrary to the fundamental principles of data protection. POPIA, South Africa's data protection legislation, defines consent to be a voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information. Unless there are additional terms and conditions made available while on the lost PIN journey, it is likely that specific and informed consent is absent when personal information is made available.

Reflections on social control

The misalignment between the privacy preserving position adopted by the app developers and the concerns raised by the technical reviewers indicate that the app is not without its flaws, and it may be contributing to some form of social control. However, this is unlikely, at least from the state's perspective. COVID Alert SA, while developed with private partners, and while certain personal information is being collected, does not appear to be a means by which the South African government is seeking to impose undue social control over people in South Africa. Downloading and using the app is not compulsory, and it is not required for accessing certain spaces.

We are however concerned that this may change as the economy continues to reopen and rebuild, and when borders open. This may prompt business owners to encourage the use of the app – although through our research we did not find any examples of businesses making the app mandatory. There is a potential concern around the current requirement to download the app if you are seeking to enter South Africa. Last year, travel agencies were encouraging travelers to install the app (Travelstart, 2020). The US Embassy travel advisory, updated in March 2021, states that travelers entering South Africa will be asked to install the COVID Alert South Africa mobile app (US Embassy, 2021). However, the most recent directions relating to air travel, published on January 29, 2021, do not mention the requirement of installing the app (Directions, 2021). While it is unclear whether this is becoming an unregulated practice or is merely advisory, we believe it is important to monitor any attempts to make the app mandatory. It will be necessary to assess any such attempts in line with the right to freedom of movement as provided in section 21 of the South African Constitution.

At this stage, it is not apparent that the app is being used by the South African government as a means of exerting unjustifiable social control. The role of the private sector in this process – both as app developers and via WhatsApp as the platform – is slightly more complicated. We acknowledge that the app developers have worked on various safeguards to ensure that privacy is protected, and these efforts should indeed be applauded; however, the concerns around the lost PIN journey and the role of WhatsApp warrant further monitoring, as some of the privacy concerns raised in this report may have been genuine oversights by the developers. The role of WhatsApp further complicates the position as it is owned by Facebook, one of the largest and most powerful social media platforms in the world. The priorities and profits motivating social media companies may not always align with efforts to advance human rights and deepen democracy. Their potentially problematic stances on privacy and data protection do raise concerns in the context of the COVID Alert SA app.

Additional app responses

Covi-ID

Privacy has been noted as a core tenet of Covi-ID. Reports explain:

> "The CoviID app will collect a user's personal location and infection status, and store it on their phone using a technology called self-sovereign identity – not on a centralised government or private-sector database. This provides the user with full authority and control over who gets access to the data, for what purpose and for how long." (Krige, 2020)

It is interesting to note that while this is a decentralized database, Covi-ID appears to collect significantly more personal information than COVID Alert SA. As detailed above, Covi-ID may collect, use, store and transfer identity, contact data, profile data, usage data and marketing and communications data. The privacy policy notes that this personal data may only be used for lawful and legitimate reasons the user must consent to. The policy further notes that it complies with, and facilitates the obligations required from, the General Data Protection Regulation, as well as POPIA.

Given that the app has not been rolled out, it is difficult to fully assess its impact from the social control perspective. However, should the app be rolled out in its current form, it may well raise data protection concerns. In terms of POPIA, personal information may only be collected if:

> "(a) the data subject or a competent person where the data subject is a child consents to the processing;
> (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
> (c) processing complies with an obligation imposed by law on the responsible party;
> processing protects a legitimate interest of the data subject;
> (d) processing is necessary for the proper performance of a public law duty by a public body; or
> (e) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied." (POPIA, section 11)

Arguably, not all the data that could be collected from Covi-ID users are necessary for the functioning of the app, and therefore it could fall short of the requirements for lawful processing.

Healthcheck

The terms of use for HealthCheck indicate that the service complies with POPIA when processing personal information (Higher Health, 2020). The consent clause states that:

> "You consent to us processing your [personal information] in accordance with the provisions of this policy in accordance with the lawful purpose. You consent to your [personal information] being processed outside of your country where necessary and to us sharing and disclosing your [personal information] for the lawful purpose."

Healthcheck collects personal information including contact numbers, location, age, gender, symptoms and exposure to infected persons, the name of the network operator and the country in which that operator is located; and details of the menu items selected. The predominant purpose for processing personal information relates to the provision of guidance and information on Covid-19 as well as conducting research and statistical analysis. Through our interview with Praekelt, we learned that Healthcheck is accompanied by comprehensive privacy notices that were drafted to be accessible to the end-user so that they are informed about how their information is collected and how it is being shared. The notices are also accompanied by an abridged version. Unlike COVID Alert SA, the use of the HealthCheck service is mandatory and controls access to higher education facilities, which raises concerns about the accuracy of the information being collected and the certainty with which conclusions may be drawn in deciding whether a student or member of staff can access the particular premises. It is worth noting that the data collected by the HealthCheck app is not anonymized (Reddy, 2020).

Assessment of alternative means

Risk-adjusted strategy and lockdown

The lockdown has led to a significant restriction on several fundamental rights. As mentioned above, a state of disaster is different from a state of emergency and does not permit a derogation of rights. As such, any limitation of constitutional rights must comply with the limitation clause contained in section 36 of the Constitution, which means that it must be reasonable and justifiable in an open and democratic society.

There have been various lawsuits filed in response to the lockdown and the risk-adjusted strategy. For instance, in *De Beer and Others v Minister of Cooperative Governance and Traditional Affairs* [2020] ZAGPPHC 184, the High Court of South Africa (per Davis J) held that the regulations promulgated by the Minister of Cooperative Governance and Traditional Affairs in terms of the DMA were unconstitutional and invalid. The judgment noted, for instance, that "[r]estricting the right to freedom of movement in order to limit contact with others in order to curtail the risks of spreading the virus is rational, but to restrict the hours of exercise to arbitrarily determined time periods is completely irrational" (para 7.8); that "to put it bluntly, it can hardly be argued that it is rational to allow scores of people to run on the promenade but were one to step a foot on the beach, it will lead to rampant infection" (para 7.9); and that "what about the poor gogo [ed. Note: grandmother] who has to look after four youngsters in a single room shack during the whole lockdown period? She may still not take them to the park, even if they all wear masks and avoid other people altogether" (para 7.10). The High Court explained further that: "During debate of the application, the argument was tentatively raised that all the limitations on constitutional rights were recompensed by the government. Counsel for the Minister had been constrained to concede that, even if the government's attempts at providing economic relief functioned at its conceivable optional best, monetary recompense cannot remedy the loss of rights such as dignity, freedom of movement, association and the like" (para 7.11). The judgment is currently on appeal.

Furthermore, in November 2020, Dear South Africa[12] launched an urgent application seeking to review and set aside the extension of the national state of disaster. According to the founding affidavit, it is claimed that there has been a derogation of rights, specifically with reference to the rights to freedom of movement,

[12] Dear South Africa is a legally recognized and constitutionally protected non-profit platform which enables the public to co-shape all government policies, amendments and proposals.

residence and assembly; economic activity; and children, family and education. It further states that: "The state of disaster grants the executive the power to pass draconian legislation that has derogated from the rights of all those who live in South Africa" and it can "be extended ad infinitum by the Minister without a requirement of Parliamentary oversight." This, Dear South Africa explains, has occurred, and continues to occur, which undermines our constitutional democracy, premised on a genuine separation of powers"(Nkosi, 2020). It is unclear at this stage when the application will be heard by the High Court.

These court cases highlight the restrictions on fundamental rights and the discontent among segments of the population regarding restrictions. At the crux of these cases has been the argument that the government has sought to impermissibly restrict fundamental rights because of the Covid-19 pandemic, in pursuit of greater control over the population and without a justifiable basis to do so.

There have also been concerns that members of the South African Police Service (SAPS) and the South African National Defence Force (SANDF) have been heavy-handed in their implementation of the lockdown regulations, resorting for instance to undue force for alleged non-compliance with the various measures. Reports note that between March and June 2020, "the number of violent incidents by police against civilians has reportedly more than doubled, with poor and vulnerable populations most affected" (Trippe, 2020). The Armed Conflict Location and Event Data Project (ACLED) recorded that the national lockdown led to a spike in heavy-handed enforcement measures (ACLED, 2020). It is with great sadness that we note the death of Collins Khosa who was viciously beaten by members of the SANDF in April 2020 at his home in the Alexandra township in Gauteng province, for what the security forces said were infringements of lockdown regulations (Rickard, 2020). In response to Mr Khosa's death, his family and their neighbors brought a case before the Gauteng High Court on May 15, 2020. In Khosa and Others v Minister of Defence and Military Defence and Military Veterans and Others [2020] ZAGPPHC 147, Judge Fabricius found that the rights to life, freedom and security, and treatment with dignity and respect were among those provided for in South African law that "may not be derogated from even in a state of emergency." He ruled that all members of the SANDF and the Johannesburg Metropolitan Police Department (JMPD) who were present or near Khosa's home should be placed on suspension. The SANDF soldiers implicated in the death of Mr Khosa have since been found to have acted improperly, irregularly and in contravention of their code of conduct, and have been disciplined accordingly (Makinana, 2020).

Efforts of the Information Regulator

Despite a limited mandate pending the enforceability of the substantive provisions of POPIA, the Information Regulator sought to provide some guidance and has called for voluntary compliance with the provisions of POPIA in the management and containment of Covid-19. In March 2020, the Information Regulator published a press statement noting that the right of access to information and the right to privacy is central to the management and containment of the spread of Covid-19 and called on the government to intensify and streamline the proactive disclosure of all information relating to the virus. The press statement noted further that:

> "The Regulator also implores health and testing centres to ensure that the personal information of everyone who has been tested and/or treated is protected. Furthermore, although [POPIA] allows the processing of information for statistical or research purposes, health and testing centres must ensure that all the other provisions of POPIA are strictly adhered to when they

test or treat patients. For instance, they must ensure that adequate safeguards are taken to ensure that the personal information is secured and is not used for any other purpose.

COVID 19 has increased the use of digital technologies such as online shopping, banking and even telemedicine in order to minimise social contact. Considering the prevalence of data breaches and cybercrime in our country and globally, the Regulator calls on both public and private bodies to increase their security measures around their digital and physical operating systems so as to protect the personal information of everyone against unlawful or unauthorised access. The Regulator supports the call by the South African Banking Association (SABRIC) to users of online services to be careful before they click on risky website links which may lure them into disclosing their personal information which might end up with cybercriminals."

In April 2020, the Information Regulator published a guidance note on the processing of personal information of data subjects in the management and containment of Covid-19. The purpose of the guidance note was two-fold: to give effect to the right to privacy as it relates to the protection of personal information; and to provide guidance to public and private bodies and their operators on the limitation of the right to privacy when processing personal information of data subjects to contain the spread and reduce the impact of Covid-19. The guidance note explained that: "The Regulator recognises the need to effectively manage the spread of COVID-19, which has necessitated the limitation of various constitutional rights of data subjects. The Information Regulator, therefore, supports the need to process personal information of data subjects in order to curb the spread of COVID-19."

Notably, the guidance note went on to set out the following conditions that must be adhered to when processing personal information of data subjects:

- Accountability, in terms of which responsible parties must process personal information of data subjects in a responsible manner during the management of Covid-19.

- Lawfulness of processing, which requires responsible parties to process the personal information of data subjects in a lawful and reasonable manner in order to detect, contain and prevent the spread of Covid-19.

- Consent, justification and objection, which makes it unnecessary for a responsible party to obtain consent from a data subject to process his or her personal information in the context of Covid-19 when processing complies with an obligation imposed by law, processing protects a legitimate interest of the data subject, processing is necessary for the proper performance of a public law duty by a public body, or processing is necessary for pursuing the legitimate interests of the responsible party or a third party to whom the information is supplied.

- Collection for a specific purpose, which requires responsible parties to collect personal information on a data subject for a specific purpose, which in this context is to detect, contain and prevent the spread of Covid-19.

- Retention and restriction of records, which obligates responsible parties to not retain records of personal information of data subjects for longer than authorized to achieve the purpose of detecting,

containing and preventing the spread of Covid-19, unless such information is required for historical, statistical or research purposes and provided that adequate safeguards are in place.

- Further processing, which allows a responsible party to further process personal information of a data subject even though such processing is not compatible with the original purpose for which it was collected if it is necessary to prevent a serious and imminent threat to public safety or public health, the life or health of a data subject or another individual, or if the information is to be used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for that purpose and will not be published in an identifiable form.
- Quality of information, which means that a responsible party should ensure that the personal information is complete, accurate, not misleading, and updated where necessary, taking into consideration the purpose for which the information was further processed.

- Documentation, which requires a responsible party to maintain the documentation of all processing operations which relate to detecting, containing and preventing the spread of Covid-19.

- Security measures on integrity and confidentiality of personal information, which requires a responsible party to take appropriate, reasonable technical and organizational measures to prevent the loss or damage to or unauthorized access to personal information. A responsible party must report any unauthorized access to personal information of a data subject to the Information Regulator and the data subjects within a reasonable time.

- Access to personal information, which obligates a responsible party to confirm whether or not it holds personal information about a data subject, upon request.

- Special personal information, which means that although a responsible party is not allowed to process special personal information, medical professionals, healthcare institutions or facilities or social services may do so if such processing is necessary for the proper treatment and care of a data subject in the context of Covid-19. In this regard, a responsible party is subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between a responsible party and a data subject.

The collection and storage of location-based data

The note from the Information Regulator goes on to provide guidance regarding the sharing of location-based data. It specifies that an electronic communication service provider may provide location-based data to the government for the purpose of managing the spread of Covid-19 – provided that the processing complies with the conditions outlined above in points c, d, and e on page 23. Furthermore, the government must still comply with the applicable conditions for lawful processing as set out in the guidance note.

Regarding mass surveillance, the guidance note provides that: "Electronic Communication Service Providers can provide the Government with location-based data of data subjects and the Government can use such personal information for the purpose of conducting mass surveillance of data subjects if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form."

The guidance from the Information Regulator was timely, given concerns around the role of digital technologies in curbing the spread of Covid-19. One of the most concerning provisions of the directions emitted under regulation 10(8) of the Regulations made under the Disaster Management Act 57 of 2002 (DCDT) allowed for what appeared to be an increased surveillance power to access location-based data, which geo-locates a mobile device and thus its user. The directions stated that relevant licensees, as well as "the internet and digital sector in general", must provide location-based data to the relevant authorities identified to support designated departments. The provision did not go further, nor did it contain a requirement of prior consent (Singh and Power, 2020). We have noted elsewhere that:

> "Location-based data has the potential to be highly sensitive and can reveal large tranches of personal information about an individual and those with whom they associate. Worryingly, there is no indication of whether this data will be anonymised or targeted, how much data will be requested, what requirements must be met for such data to be accessed or what safeguards will be in place to access such data, including whether a judicial order will first have to be obtained before the data can be acquired. In the absence of appropriate public consultation, there has also not been an opportunity to ventilate what the exact purpose of this measure is, or whether there is appropriate evidence supporting its efficacy. Indeed, the current public health crisis should not warrant an excessive criminal justice response. It seems inevitable that a re-drafting or clarification will urgently be required, because this provision may constitute a step backwards in relation to privacy rights protections if not appropriately circumscribed and implemented." (Singh and Power, 2020)

A group of prominent academics suggested that "the Tracing Database initiative occupies an emerging global regulatory space, at the intersection of public health, constitutional rights during emergencies and disasters, credit surveillance, open data, and information privacy" (Klaaren et al., 2020). The group issued an important caution, relevant for our understandings around issues of social control:

> "Fundamentally we argue that while the public may tolerate this degree of invasion of privacy under particular circumstances, there is a danger that it will become normalised, and the exceptional nature of infringements of individual rights needs to be underscored. Public debate, participation, and education on these privacy and ethical issues is important in a rights-based constitutional democracy."

Had the directions not been amended shortly after they were published, it is likely that privacy, surveillance, and social control concerns would have been amplified. Fortunately, the "controversial proposal to track people using their phones and other devices in the bid to contain Covid-19" was not pursued (Hunter and Thakur, 2020). The Right to Know Campaign (R2K) published a useful explanatory note which explained that the state cannot share personal information to the Police and State Security Agency as these bodies were not included as part of the process. R2K also noted that the state should ensure that no person's data from before March can be sought about their movements, whether they tested positive for Covid-19 or not, and that no person's data can be sought after the national disaster. These measures, along with the designated judge and increased transparency, alleviated some of the serious concerns regarding social control (R2K, 2020).

Regulation of disinformation

There is no doubt that mis- and disinformation present a serious challenge to efforts to curb the spread of Covid-19. According to experts, there has been a significant rise in false information peddling amid the Covid-19 pandemic – including for instance senior politicians and members of the judiciary expressing their doubts about the role of Covid-19 vaccines and the management of the pandemic (Smith, 2021). For example, in December 2020, Chief Justice Mogoeng Mogoeng remarked during a prayer that "[i]f there be any vaccine that is of the devil, meant to infuse triple-six in the lives of people, meant to corrupt their DNA, any such vaccine, Lord God almighty, may it be destroyed by fire, in the name of Jesus." Many felt that this statement was false, dangerous and could lead to unfounded fears around vaccine safety (Seleka, 2021).

In 2020, the South African Police Service (SAPS) shared views relating to the disinformation of content that was unrelated to Covid-19. For instance, in a media statement the Office of the Provincial Commissioner in the Eastern Cape stated that: "Any person who publishes, distributes, discloses, transmits, circulates or spreads false information or fake news is guilty of an offence and may be prosecuted" (SAPS, 2020). And in another media statement, the same office indicated that: "Members of the public and particularly those who hold public offices are warned not to make unsubstantiated and inflammatory statements which have a potential to create instability and uncertainty within the communities. It must be noted that spreading fake and fabricated information to sow confusion and harmful anxiety to the people may lead to prosecution. This behavioural conduct cannot be tolerated during this critical time in our country" (SAPS, 2020). However, this broad interpretation does not cohere with the actual text of the offence created in terms of the regulations, which is more narrowly circumscribed.

The challenge that this presents is that although individuals may not actually be convicted in terms of this provision, the harm is already caused through fear of falling foul of the provision, resulting in self-censorship on matters that may be of public importance. There is also a real concern that, going forward, there may be more regulatory measures proposed in an effort to regulate so-called fake news more generally through the imposition of criminal sanctions.

There is currently no legislation in South Africa that makes disseminating disinformation a general offence. However, under regulations published by the Department of Cooperative Governance and Traditional Affairs (CoGTA) in terms of the DMA, a new criminal offence was created for the dissemination of fake news pertaining to Covid-19. Specifically, the regulations prohibit the publication of any statement, through any medium, including social media, with the intention to deceive any other person about Covid-19, the Covid-19 infection status of any person, or any measure taken by the government to address Covid-19.

Furthermore, in terms of the directions published by the Minister of Communications and Digital Technologies on March 26, 2020, licensees, over-the-top services (OTTs) and internet service providers (ISPs) are to remove fake news related to Covid-19 from their platforms immediately. The directions do not provide any clarity regarding who has authority to issue an instruction for the removal of content, or what recourse an affected person may have if content has been wrongfully removed.

Civil society and activists have warned against clamping down on the right to freedom of expression through the criminalization of mis- and disinformation relating to Covid-19. In April 2020, the R2K Campaign wrote to

the Minister of CoGTA on behalf of the C19 Peoples' Coalition,[13] highlighting the chilling effect that criminal provisions have on the exercise of the right to freedom of expression, and urging the government to adopt a more tempered approach in line with the Constitution (R2K, 2020). Similarly, the International Commission of Jurists, for example, has noted that these provisions are broad, with various challenges relating to their enforceability, and has questioned whether the provisions may indeed be unconstitutional when tested against the right to freedom of expression contained in section 16 of the Constitution (News24, 2021).

There have also been non-governmental responses to disinformation. For example, the Centre for Analytics and Behavioural Changes (CABC) at the University of Cape Town launched a six-month project aimed at combatting the dissemination of dis- and misinformation relating to Covid-19 (News24, 2020). Furthermore, the Real411 platform was launched by Media Monitoring Africa to enable members of the public to report concerns regarding disinformation, hate speech, incitement to violence and harassment, and was formally endorsed by the government in April 2020:

> "A hi-tech monitoring and evaluation process has been put in place to assess complaints and reports from the media, the public and other sectors of society, with the ability to take down fake news items on a range of platforms and submit cases to the SAPS for investigation and prosecution.
>
> This solution is a unique collaboration between the Department, the Government Communication & Information System, Media Monitoring Africa and the CovidComms volunteer communication network. It forms part of the work of a special Ministerial Task Team established by the Department of Communications & Digital Technologies, which also includes representatives from ICASA, Film & Publications Board, ZADna, mobile phone companies and other key players in the ICT sector, including platform owners.
>
> Once fake news items or social media posts have been identified, platform owners are notified to bring down the posts. Electronic Communications Services Licensees, including over-the-top media service providers and internet service providers that are in the service of providing linear and non-linear services, will then have the responsibility to remove fake news from their platforms with immediate effect." (PoliticsWeb, 2020)

The Information Regulator has also weighed in, noting in a press statement in March 2020 that: "Whilst we recognise the important role played by social media in the dissemination of information relating to COVID-19 in real-time, we advise the government to engage social media companies and request them to subject all information relating to the virus on their platforms to third-party fact-checking programme and remove fake news and disinformation from in their platforms."

While responding to mis- and disinformation regarding Covid-19 is imperative, it is equally important to ensure that an appropriate balance is struck with the right to freedom of expression. The current approach of making spreading false information relating to Covid-19 a criminal offence, coupled with a disjointed approach of parallel directions published by the Minister of Communications and Digital Technologies, creates a

[13] The C19 People's Coalition is an alliance of social movements, trade unions, community organizations and NGOs united in the struggle for a just and effective response to the COVID 19 pandemic through building resilient, informed and organized communities. They are committed to ensuring that the South African response to the COVID-19 virus is effective, just, equitable, and meets the needs of the most marginal in our unequal country.

framework that is confusing and unclear, and that may have a chilling effect on the right to freedom of expression. It is of particular concern that neither the regulations published in terms of the DMA nor the directions published by the Minister of Communications and Digital Technologies were subject to parliamentary oversight or public consultation, despite the severe limitation that they present to the right to freedom of expression.

Assessment of combined alternative means and app responses

COVIDConnect

One of our interviewees, digital rights activist Murray Hunter, explained that it has been difficult to obtain detailed information about COVIDConnect. This correlates with our experience in accessing further details about the platform, including what data is collected, stored, and processed. We experienced challenges accessing the privacy policy as it was only available to people who had initiated conversations with the WhatsApp chatbot. From our understanding, it appears that COVIDConnect relies on the NDOH COVID-19 USSD and WhatsApp Service privacy policy, which is the same as the HealthCheck privacy policy. The policy states that the following personal information can be directly collected from users:

- If you communicate with the NDOH using the Service, we will receive your phone number and WhatsApp username if via WhatsApp.
- If you use any of the self-diagnosis features on the HealthCheck Channel we will receive the information that you submit in your responses. The PI that may be collected is in response to the following questions:
    - Location (Province and Town or Location Pin). You don't have to provide us with location information. If you choose to tell us your location, we will collect that information
    - Age category
    - Gender
    - Symptoms: fever, cough, sore throat, difficulty breathing, body aches, loss of taste or smell
    - Exposure to infected persons
    - Existing underlying medical conditions
- If you send messages to the Service, we will receive the information that you include in your message.

The name of a user's network operator and the country in which the network operator is located, as well as the details of the menu items users select, is automatically collected and recorded. The policy then notes that that communications using WhatsApp are secured with end-to-end encryption, which means that WhatsApp and other third parties cannot read or access them, and refers users to the WhatsApp privacy policy. The policy provides reasons as to why personal information is collected, including: for the provision of guidance and information, for public health and safety purposes, for conducting research and statistical analysis, improving services, and keeping the channel safe and secure. The policy explicitly states: "[w]e will not publish or sell any personally identifiable information."

The launch of COVIDConnect does not appear to have been nefarious. Hunter explains that "[t]here is no evidence that this system has been designed with malicious purposes and in fact, in many ways, the

regulations [relating to contact tracing] that have been drafted, were very clearly sensitive to the privacy concerns people were raising" (Voigt, 2020).

However, there are some concerns worth exploring. One of Hunter's key concerns related to the lack of input, information, public consultation and information about how they were going to implement COVIDConnect. Security issues were also raised. Professor Co-Pierre Georg, one of the Covi-ID developers, noted that the problem with this combination of data, health data, location data, and identity data collected by COVIDConnect is that it makes it very attractive for hackers (Voigt, 2020). Professor Georg has gone as far as to say that "COVIDConnect is not a contact tracing tool, but a political stunt by the minister to distract from his previous failure to develop a digital contact tracing system" (Georg, 2020). Razzano remarked that COVIDConnect was launched by the government seeking to leverage an existing political success (that of MomConnect, a WhatsApp-based maternal health support platform) though a technological approach (Razzano, 2020).

The project team from Praekelt and the NDOH have responded to concerns about COVIDConnect, stating that the security of data has been a "priority of all parties involved in the programme throughout the various phases of the programme" (Voigt, 2020, quoting Rogers of Praekelt). We were advised during our interview with Praekelt – one of the partners working on COVIDConnect and HealthConnect – that they have placed significant emphasis on privacy and data protection. They explained that when someone is using the COVIDConnect platform, there is an abridged privacy policy that leads to a full privacy policy that sets out what data is collected and in terms of which legislation, as well as who it is being shared with. Praekelt explained further that they worked on ensuring that the policies would be accessible for most users. The NDOH has advised that COVIDConnect has end-to-end encryption to protect personal information, and the platform has received legal and ethical clearances from health research ethics committees (Voigt, 2020).

Some consideration has been given to various privacy concerns. However, a key issue, which has not been raised elsewhere and came to light in our engagements with the technical reviewers, relates to the concerns listed about the use of WhatsApp as a platform. To reiterate, the technical reviewers note that the use of WhatsApp raises privacy concerns, particularly because of the commercial interests of third parties.

WhatsApp is incredibly popular in South Africa. It is used both by the general public and by the South African government to communicate with people. GovChat, South Africa's largest online civic engagement platform, uses WhatsApp. However, and to echo the concerns of the technical reviewers, convenience alone is not a sufficient justification to outweigh privacy concerns. Studies have shown that even though WhatsApp is popular with healthcare professionals, its privacy concerns render it an inappropriate platform on which to share healthcare information (Masoni and Geufli, 2020). In the United States, healthcare professionals have been advised to abandon WhatsApp and move towards secure messaging apps in order to maintain confidentiality and ensure the security of patient data. Interestingly, there was a significant uproar in South Africa against WhatsApp's proposed privacy policy updates (McKane, 2021). However, despite the backlash there appeared to have been little concern expressed about COVIDConnect.

We are concerned that limited attention has been given to this issue. WhatsApp is part of a powerful social media company whose interests and priorities are likely to be predominantly profit-driven, rather than focused on protecting privacy. We are therefore concerned that its sustained use may jeopardize the privacy and data protection rights of those who use COVIDConnect. In relation to the recently proposed privacy policy updates to WhatsApp, the South African Information Regulator has found:

> "[P]rocessing of cellphone numbers as accessed on the user's contact list for a purpose other than the one for which the number was specifically intended at collection, with the aim of linking the information jointly with the information processed by other responsible parties (such as Facebook companies) does not require consent from the data subject, but prior authorisation from the Information Regulator. Accordingly, WhatsApp cannot without obtaining prior authorisation from the Information Regulator in terms of section 57 of Protection of Personal Information Act (POPIA) process any contact information of its users for a purpose other than the one for which the number was specifically intended at collection, with the aim of linking that information jointly with information processed by other Facebook companies." (Information Regulator, 2021)

While this does not address all the forms of personal information currently collected through COVIDConnect, it is hoped that this statement from the Information Regulator, coupled with growing awareness around WhatsApp's privacy positions, will prompt further engagement with and critique of COVIDConnect. Although considerations around social control in relation to COVIDConnect are not glaringly apparent, the fact that a platform owned by a powerful social media company is being used to collect vast quantities of personal information, including sensitive personal health information, continues to be of concern.

PILLAR 3: CONTACT TRACING APPS (MOBILITY FEATURES) AND FUNCTION CREEP – IMPACT ON EQUAL ACCESS AND PARTICIPATION OF VULNERABLE PERSONS IN SOUTH AFRICA

Assessment of app response

COVID Alert SA

At the outset of this research, before the release of COVID Alert SA, we were concerned that exclusion or discrimination based on nationality would be a key issue. South Africa is notorious for xenophobic harassment and violence against African and Asian foreigners living in the country (Human Rights Watch, 2020). Throughout 2020, amid widespread economic decline, devastating unemployment levels, and increased levels of crime, there were concerted attempts, through protests and social media campaigns, to stoke the fire against foreign nationals (Meyer, 2020). The South African government has often blamed undocumented foreigners for medical shortages, using non-nationals as scapegoats for economic insecurity and the government's service delivery failures (Shoba, 2020). We were therefore concerned that the government might use a tech-based solution to Covid-19 to track foreign nationals. However, this did not turn out to be the case as COVID Alert SA does not appear to exclude or discriminate against foreign nationals. Furthermore, the app does not appear to contribute disproportionally to the vulnerability of foreign nationals in South Africa.

Our second concern was related to journalists. This concern stems from a case in which a prominent investigative journalist, Sam Sole, had been the subject of state surveillance. Sole, along with AmaBhungane Centre for Investigative Journalism, approached the courts alleging that South Africa's surveillance legislation – RICA – was unconstitutional as it fails to provide adequate safeguards to protect the right to privacy. Given this prior incident of surveillance of a journalist, we were concerned about the possibility of an app-based solution being used to track and surveil members of the media. However, following an interview with Sam Sole, and other journalists and freedom of expression experts, it was clear that this concern was unfounded.

Notably, issues of access, connectivity, data prices, and the digital divide were raised in nearly every interview we conducted. South Africa ranks as the continent's best-performing country in the Inclusive Internet Index for 2020 (Inclusive Internet Index, 2020). Unfortunately, this laudable ranking does not mean that access and connectivity are a reality for all. Approximately 63% of people in South Africa are internet users; however, it appears that only 10.4% of South African households can access the internet at home, and for people living in rural areas this figure drops to 1.7% (Statista, 2020; StatsSA, 2018). 60.1% of people use mobile devices to access the internet. Following the 2019 recommendations of the Competition Commission that data prices in South Africa were too high and pricing structures "anti-poor", there have been efforts to reduce the cost of

data to advance accessibility (Competition Commission, 2019; Independent Communications Authority of South Africa (ICASA), 2020). However, according to Research ICT Africa:[14]

> "Despite recent mandatory data price reductions by the dominant operators, data pricing in South Africa remains high. According to The State of ICT in South Africa report, most South Africans cannot afford to go online due to data costs, lack of internet-enabled devices and digital literacy, all of which are associated with poverty, which are the main barriers to getting online. Research ICT Africa's Retail African Mobile Pricing (RAMP) Index, shows that South Africa performs poorly amongst other African countries, ranking 33rd out of 46 countries in terms of data per gigabyte (GB) costs, as at 2020Q1. Since we do not expect altruism by mobile network operators, it is therefore important to understand that the reduction in mobile tariffs was not in response to the COVID-19 pandemic, but a compliance to the Competition Commission Data Services Market Inquiry."

Research ICT Africa notes further that due to lack of regulation and an inherently imperfect market, even after the reduction, prices remain anti-poor (Research ICT Africa, 2020).

There are also challenges regarding digital literacy. For those who can get online and make use of online services – such as the information portals and applications provided in response to Covid-19 – there remain risks about whether they are able to do so safely and securely.

The app developers explained that they sought to be mindful of data cost concerns in South Africa. Accordingly, the download size is under 10MB, the app is free and does not feature in-app purchases. Once downloaded and installed COVID Alert SA runs in the background. It is worth noting that the app only works on certain operating systems that need to have been recently updated. It appears that an update to Google Play Services would take up around 45MB. Research ICT Africa noted that although it appears to be a relatively low-cost data application, "COVID Alert is a public health instrument to contain the virus and there should not be cost considerations for the public to use it" (Research ICT Africa, 2020). A further point to note is that a smartphone is needed to download the app. While smartphone penetration sits at 91.2%, it is estimated that just one-third of the country's population are smartphone users (ICASA, 2020; Statista, 2020).

There has arguably been ineffective communication around how the app works. Judge O'Regan suggested that communication is one of the key areas in which there is room for improvement. Members of the Praekelt team noted that getting substantial uptake of the app would be challenging given issues around access to mobile phones and data. They noted that there will likely be challenges related to users understanding how the app works, noting that it is a complicated concept, and people may mistrust it if they do not fully understand it.

The app is currently only available in English even though South Africa has 11 official languages, of which English is the sixth most common spoken in the home, and the second most spoken outside the home (General Household Survey, 2018). isiZulu and isiXhosa rank highly both as home languages and languages spoken outside the household. When engaged on this issue the app developers noted the concerns and indicated that there is a possibility of making the app available in other languages.

[14] Research ICT Africa, an ICT policy and regulation think tank, is a not-for profit organization under section 21 – REG NO. 2009/017831/08 – PBO NO. 930034057

The above points highlight that while the NDOH and the app developers have tried to ensure degrees of inclusivity, some barriers to access affect people disproportionally, largely based on their socio-economic status. Therefore, addressing data costs, challenges around digital literacy, and language barriers would assist in lessening the impact on unequal access and participation.

Additional app responses

According to one of the developers of Covi-ID, you would need some data to access and download the QR code. She explained that it is 75KB to download. There do not appear to be any built-in functions that advance usability, mobility and accessibility. The availability of Healthcheck on USSD is notably inclusive from an access perspective and allows those without access to airtime or the internet to use the service. The HealthCheck digital risk-assessment and mapping tool is set to be available in all 11 official languages, starting with English, isiZulu, isiXhosa, seSotho and Afrikaans (Turn, 2020).

Assessment of alternative means

Unlike the tech-based responses, which in the main have not been extremely problematic for vulnerable groups, the alternative means have been quite concerning. The lockdown in particular has had a considerable impact on serval vulnerable groups, including people who are homeless, people living in informal settlements, women, children, gender and sexual minorities, and foreign nationals.

Limited forms of formal and informal income, insufficient water supply, and constrained spaces in informal settlements are but a few of the many challenges faced by many indigent people in South Africa whose lived realities were compounded by Covid-19 (Simelane, 2020). The use of quarantine camps has been a contentious issue in South Africa. In May 2020, AfriForum[15] won a case regarding the use of Covid-19 quarantine camps, in terms of which the High Court ruled that the camp where over 100 people were being held should be closed immediately. According to AfriForum:

> "AfriForum will not tolerate such abuses of power by government officials. It is immoral that people are detained in such camps and that officials refused to test them for such a long time. It is a blatant violation of people's basic freedoms. These people were prisoners for all intents and purposes. The facility not only violated the required WHO standards, but the people were also kept there against their will … These cases prove that the national regulations – which allow the government to force people into quarantine camps, regardless of whether they can effectively self-isolate – are irrational. It is a violation of the most basic freedoms and dignities of people and amounts to measures that can under no circumstances be justifiable in any democracy." (AfriForum, 2020)

Mukumbang explains that "[w]hile these containment measures are estimated to have negatively affected all those living in SA, asylum-seekers, refugees, and undocumented migrants disproportionally experience the negative impacts of the pandemic because of existing vulnerabilities affecting this population." Organizations

[15] AfriForum is a non-governmental organization – registered as a non-profit company – with the aim of protecting the rights of minorities. While the organization functions on the internationally-recognized principle of the protection of minorities, AfriForum specifically focuses on the rights of Afrikaners as a community living on the southern tip of the continent. Membership is not exclusive, however, and any person may join who can associate themselves with the contents of the Civil Rights Manifest of the organization.

working with foreign nationals during the lockdown indicated that there was a spike in their arrest and detention. They were more likely to be arrested for minor offences and less likely to be released on bail because of expired documentation. Documentation renewal became complicated and unsettling for many when the Department of Home Affairs office closed during the lockdown. In addition to these challenges, Mukumbang records that foreign nationals are less willing to seek testing or care for Covid-19 symptoms as they are afraid of being detained or deported (Mukumbang et al., 2020).

Sex workers also faced a plethora of challenges as South Africa entered lockdown. The already tense relationship between sex workers and the police (SAPS) worsened during the lockdown, with sex workers experiencing intensified harassment and arrest (Smit, 2020).[16] The sex work industry took a significant blow, as customers were concerned about contracting the virus, and accessing sex work became harder with increased police presence and curfews. Sex workers also reported interruptions to condom supplies (Soer, 2020).

Disproportionate gender-based burdens, economic vulnerability, and heightened safety concerns left women and gender and sexual minorities in a difficult position (Parry, 2020). In an unprecedented speech, President Ramaphosa expressed his anger at the men of the country who were perpetrating violence against women during the pandemic. Some of his remarks are recorded below:

> "Over the past few weeks, no fewer than 21 women and children have been murdered. Their killers thought they could silence them. But we will not forget them, and we will speak for them where they cannot."
>
> "As a country, we find ourselves in the midst of not one, but two, devastating epidemics. Although very different in their nature and cause, they can both be overcome – if we work together, if we each take personal responsibility for our actions and if we each take care of each other."
>
> "It is with the heaviest of hearts that I stand before the women and girls of South Africa this evening to talk about another pandemic that is raging in our country – the killing of women and children by the men of our country."
>
> "As a man, as a husband and as a father, I am appalled at what is no less than a war being waged against the women and children of our country."
>
> "At a time when the pandemic has left us all feeling vulnerable and uncertain, violence is being unleashed on women and children with a brutality that defies comprehension. These rapists and killers walk among us. They are in our communities. They are our fathers, our brothers, our sons and our friends; violent men with utterly no regard for the sanctity of human life." (Ramaphosa, 2020)

The above examples are but a handful of the experiences of vulnerable individuals and communities in South Africa. The lockdown undoubtedly had a significant impact across the board with many still facing threats to their livelihood, threats to their safety, and threats to their health.

[16] Sex work is currently illegal in South Africa.

Assessment of combined alternative means and app responses

CovidConnect

During our research and interviews, we did not uncover any particular discriminatory or exclusionary practices associated with CovidConnect, save for issues around access and digital literacy – similar to the challenges described above.

While CovidConnect appears to be the most used of the tech-based tools, it is still not accessible to everyone. Razzano explained that 30 to 40% of people in South Africa do not use WhatsApp, and even though using the portal costs very little, it does require airtime or data. She explained that "[y]et again, the realities of South Africa's digital inclusion, and the mechanics of human engagement, were underappreciated in the implementation of a solution, which preferred an already entrenched public-private partnership" (Razzano, 2020).

Similarly, we are concerned about the extent to which people whose information is being collected and shared are appropriately informed of the uses of this information. Although COVIDConnect is premised on consent, we are concerned that this is not written in easily accessible language, and that people may feel compelled to provide personal information without knowing that this is not required. It is also of concern that people making use of this service are not only providing their own personal information but that of other people who they have been in contact with – without necessarily obtaining their consent before doing so.

Notably, CovidConnect is available in Sotho, Zulu, Afrikaans and Xhosa, and English. Once on the platform, a user can select the language of their choice before moving to the main menu of options.

A welcome development, while not directly linked to COVIDConnect, was the regulations that provided for zero-rating health and educational sites by mobile network operators, such as MTN and Vodacom (Amendment of ICT COVID-19 National Disaster Regulations, 2020;. As of July 2020, there were 988 zero-rated websites in South Africa (Parliamentary Monitoring Group (PMG), 2020). Additionally, ICASA issued a temporary radio frequency spectrum to deal with Covid-19 communication challenges (ICASA, 2020), subject to certain licensing conditions which included the obligation to provide data services at a reduced rate to consumers, zero-rating and connecting virtual classrooms free of charge (PMG, 2020).

CONCLUSION AND RECOMMENDATIONS

One of the key learnings from this research is that digital solutions to contact tracing, while important and useful, are not a silver bullet to respond to a public health crisis. It remains necessary to combine digital solutions with other measures to effectively reach the majority of the population. For example, the NDOH has described the use of the COVID Alert SA app as having "mixed results": on the one hand, it can be a key mechanism for those who have access to a smartphone, understand the implications of using the app, and are familiar with concepts such as zero-rating; on the other, it can result in exclusionary consequences for those who fall outside of this realm.

It is also apparent that the development of digital solutions must be accompanied by the necessary supporting and enabling environment. Where digital solutions are intended to be used on a wide scale by, for example, community healthcare workers, this can only be successful if there is appropriate resourcing, training, and provision of equipment. The failure to meet any one of these three requirements may result in an overall failure to roll out and implement such programs.

Additionally, and while it is difficult to fully know the effectiveness of South Africa's risk-adjusted strategy and the early lockdown intervention, it is likely these measures were helpful particularly from a public health perspective. Efficacy varied across the regulations and directions that came from the Disaster Management Act, as well as the public communications published, with some providing useful and meaningful guidance on key issues such as the risk-adjusted strategy, whereas others, particularly in the early days of the lockdown, were of concern but fortunately promptly changed. Overall, despite some apprehension and challenges, we are of the view that electing to deal with Covid-19 through the framework of the Disaster Management Act rather than declaring a state of emergency was a far better approach from a human rights perspective.

As a general proposition, the NDOH and other government bodies appear to have taken privacy seriously when developing contact tracing solutions to contain the pandemic. The safeguards contained in the Amended Regulations published in terms of the DMA are particularly noteworthy, including the provisions for user notification, limited retention periods and ongoing reporting. A highlight was the appointment of a credible judge to oversee the process and ensure transparency and accountability in the implementation of the contact tracing database.

However, there have also been several concerns. For a well-functioning constitutional democracy, it is imperative that there is parliamentary oversight, public consultation, and engagement on any measure that will limit fundamental rights, including the right to privacy. While one can understand the challenges occasioned by a pandemic, these elements were starkly lacking to the detriment of the efficacy, and arguably the constitutionality, of the measures implemented.

To some extent, these challenges could have been ameliorated if there had been proper public consultation. While it is our understanding that the government did indeed approach reputable legal and other experts in the development of the Amended Regulations on contact tracing, as well as for the COVID Alert SA app, a wider consultative process could have harnessed better results, mitigated the shortcomings, and gained more trust from the public. While the government has been afforded significant leeway to respond to Covid-19 quickly without public consultation, a more consultative approach could have avoided some of the court

challenges and failed efforts, including the COVIDConnect measures with the telecommunications operators that ultimately proved ineffective.

This speaks more broadly to some of the underlying challenges, and the extent to which the decisions regarding contact tracing were based on research and data-driven considerations. For instance, it is apparent that reliance on telecommunications operators to provide location-based and other data in South Africa was ill-considered and ineffective. Although it should be welcomed that this was quickly abandoned, it was allowed to persist for a period during which vast amounts of personal information were being shared between the private sector and the government. Added to this, it appears that the rollout of the COVID Alert SA app drew heavily on a University of Oxford study, designed for the rollout of contact tracing apps in the United Kingdom. This ignores the stark differences between the United Kingdom and South Africa, including internet penetration, digital literacy, and access to devices. Similarly, the reliance on WhatsApp as a communications platform for the government has been cause for concern: a significant portion of the population does not use this platform, with this number having grown following the proposed changes to WhatsApp's terms of service that has resulted in many people leaving the platform out of concern for their privacy.

From an oversight perspective, it is a concern that the Information Regulator has not been involved in discussions regarding contact tracing, despite the obvious privacy considerations that arise. While one might posit that this is because of the limited mandate of the Information Regulator pending the full enforcement of POPIA, this in itself is not sufficient to justify the complete exclusion of the privacy regulator. The role assigned to Judge O'Regan is an important, albeit limited, one – and indeed there has been little public reporting regarding the reports and directions provided to or by the designated judge – whereas the Information Regulator would be well-placed to consider the privacy implications of the various contact tracing measures more holistically had the office been properly involved and consulted.

Added to this, communication regarding the contact tracing measures has been inconsistent and relatively poor. This may result in a lack of trust in the measures, which would diminish their efficacy. For instance, it is difficult to ascertain precisely who has access to the COVIDConnect database, with whom the information contained in this database is shared, or what security measures are undertaken to safeguard personal information.

Considering the above, we propose the following recommendations:

- **Recognition of the impact of Covid-19 responses on various rights**: The government should conduct short-, medium- and long-term evaluations in which they reflect on success, challenges, and mistakes. An important component of this relates to the type of legal framework that has guided the government's approach. In future crises, human rights impact assessments should inform the legal framework, including reflections on states of emergency and states of disaster, and what would be necessary and justifiable in the given situation.

- **Privacy is key**: The government, and any private partners it may work with, must ensure rights-based and transparent regulatory and policy frameworks that guide technical responses to Covid-19, with a particular emphasis on privacy rights. Government, and its partners, must urgently re-assess the use of WhatsApp as part of its response to Covid-19. Activists, academics, and members of the technical community should conduct further research on this point and support the government in finding safer and more appropriate options and solutions.

- **Access**: The government must take urgent steps to enable the establishment and use of Universal Service and Access Funds and Digital Inclusion Initiatives and Funds to ensure that people in South Africa can access relevant response resources and services. Further efforts to establish zero-rate information portals are encouraged.

- **Digital literacy**: Digital materials must be developed and made accessible. These materials must be clear and appropriate, accompanied by training and tools that address how to use the relevant app as well as highlighting key data privacy issues. Digital literacy training should be provided to government staff, community health workers, and app users.

- **Communication**: Focused and targeted communication efforts should continue. Everyone in South Africa should be provided with access to accurate and timely information about Covid-19, COVID Alert SA, COVIDConnect, and any other measure that requires any personal information to be collected and processed. The media must comply with applicable codes of conduct, the South African Constitution, and international human rights standards to ensure that information disseminated is true, accurate and fair. The media is encouraged to engage with other sectors, specifically academia, the technical community, and civil society to publish information that informs people of relevant Covid-19 developments.

- **Consultation**: The government must, as much as reasonably practical, quickly and without delay ensure public consultation on key developments and measures.

- **Oversight and review mechanisms**: The Information Regulator must be involved in discussions regarding contact tracing and the government should facilitate meaningful engagements with key stakeholders. In line with Judge O'Regan's recommendations, the government should undertake independent security audits of the systems it has authorized.

REFERENCE LIST

Legal frameworks

Amended Regulations in terms of the Disaster Management Act, April 2, 2020 (accessible at https://powersingh.africa/wp-content/uploads/2020/04/COVID-19-Amended-Regulations-issued-in-terms-of-the-Disaster-Management-Act-2002-2-April-2020.pdf).

Directions on measures to prevent and combat the spread of COVID-19 in the air services for adjusted alert level 3 (January 28, 2021) (accessible at https://www.gov.za/sites/default/files/gcis_document/202101/44124gon63.pdf)

Directions on Zero-Rating of Websites for Education and health issues under regulation 4(10) of the Regulations made under the Disaster Management Act, 2002 (Act 57 of 2002) (accessible at https://www.gov.za/sites/default/files/gcis_document/202006/43411gon651.pdf)

Disaster Management Act 57 of 2002

Electronic Communications, Postal and Broadcasting Directions issues under the Disaster Management Act, March 26, 2020 (accessible athttps://www.gov.za/sites/default/files/gcis_document/202003/43164gon-417.pdf)

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

All regulations, directions and guidelines relating to COVID-19 in South Africa can be accessed here: https://www.gov.za/covid-19/resources/regulations-and-guidelines-coronavirus-covid-19#

Case law

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others [2021] ZACC 3 (accessible at http://www.saflii.org/za/cases/ZACC/2021/3.html)

De Beer and Others v Minister of Cooperative Governance and Traditional Affairs [2020] ZAGPPHC 184 (accessible at http://www.saflii.org/za/cases/ZAGPPHC/2020/184.html)

Research reports, policies, and statistics

ACLED, "CDT spotlight: South Africa" (2020) (accessible at https://acleddata.com/2020/06/04/cdt-spotlight-south-africa/)

Competition Commission Data Services Market Inquiry (2019) (accessible at http://www.compcom.co.za/wp-content/uploads/2019/12/DSMI-Non-Confidential-Report-002.pdf)

Covi-ID, "Privacy and Personal Information Policy" (2020) (accessible at https://docs.google.com/document/d/19u3WE-w5VfNNyxQrYmZxsRRHH-WY0VbfE1eMmxRf9rQ/edit)

Department of Public Health, "COVID-19 Online Resources and News Portal" (2020) (accessible at https://sacoronavirus.co.za/)

Higher Health, "Higher Health COVID-19 USSD, Whatsapp & Web Service Privacy Policy" (2020) (accessible at https://healthcheck.higherhealth.ac.za/terms/)

HSRC, "Tuberculosis in the context of the COVID-19 pandemic in South Africa" (2020) (accessible at http://www.hsrc.ac.za/en/news/general/TB-covid-19)

Hunter, "Track and trace, trial and error. Assessing South Africa's approaches to privacy in Covid-19 digital contact tracing" (2020) (accessible at https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/track-and-trace-digital_contact-tracing-in-sa-nov-2020.pdf)

ICASA, "Temporary radio frequency spectrum issued to qualifying applicants in an effort to deal with COVID-19 communication challenges" (2020) (accessible at https://www.icasa.org.za/news/2020/temporary-radio-frequency-spectrum-issued-to-qualifying-applicants-in-an-effort-to-deal-with-covid-19-communication-challenges)

ICASA, "The State of the ICT Sector Report in South Africa" (2020) (accessible at https://www.icasa.org.za/uploads/files/State-of-the-ICT-Sector-Report-March-2020.pdf)

Inclusive Internet Index 2020 (2020) (accessible at https://theinclusiveinternet.eiu.com/explore/countries/ZA/)

Independent Communications Authority of South Africa (ICASA), "Communications & Digital Technologies Ministry and ICASA welcome steps taken by the Competition Commission to facilitate data prices reduction at the retail level of the market" (2020) (accessible at https://www.icasa.org.za/news/2020/communications-digital-technologies-ministry-and-icasa-welcome-steps-taken-by-the-competition-commission-to-facilitate-data-prices-reduction-at-the-retail-level-of-the-market)

Information Regulator, "COVID-19" (2020) (accessible at https://www.justice.gov.za/inforeg/media.html)

Information Regulator, "Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA)" (2020) (accessible at https://www.cgcsa.co.za/wp-content/uploads/2020/04/Information-Regulator-Guidance-Note-Covid-19.pdf)

International Monetary Fund (IMF), "Six Charts Explain South Africa's Inequality" (2020) (accessible at https://www.imf.org/en/News/Articles/2020/01/29/na012820six-charts-on-south-africas-persistent-and-multi-faceted-inequality)

Klaaren et al., "South Africa's COVID-19 Tracing Database: Risks and rewards of which doctors should be aware" *Medicine and the Law* (2020) (accessible at http://www.scielo.org.za/pdf/samj/v110n7/18.pdf)

Little et al., "Yield of household contact tracing for tuberculosis in rural South Africa" (2018) 18 *BMC Infectious Diseases* (accessible at https://bmcinfectdis.biomedcentral.com/articles/10.1186/s12879-018-3193-7).

Masoni and Geufli, "WhatsApp and other messaging apps in medicine: opportunities and risks" (2020) 15 *Internal and Emergency Medicine* (accessible at https://link.springer.com/article/10.1007/s11739-020-02292-5)

Mukumbang et al., "Unspoken inequality: how COVID-19 has exacerbated existing vulnerabilities of asylum-seekers, refugees, and undocumented migrants in South Africa" (2020) 19 *International Journal for Equity in Health* (accessible at https://equityhealthj.biomedcentral.com/articles/10.1186/s12939-020-01259-4)

O'Neil, "No, coronavirus apps don't need 60% adoption to be effective" *MIT Technology Review* (2020) (accessible at https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/)

Parliamentary Monitoring Group (PMG), "Political Party Representation in National Assembly" (2019) (accessible at https://pmg.org.za/page/political-party-representation)

Parry, "The shadow pandemic: Inequitable gendered impacts of COVID - 19 in South Africa" (2020) *Feminist Frontiers* (accessible at https://onlinelibrary.wiley.com/doi/full/10.1111/gwao.12565).

PMG, "Question NW1245 to the Minister of Communications" (2020) (accessible at https://pmg.org.za/committee-question/14312/)

Praekelt, "COVID-19 Connect South Africa" (2020) (accessible at https://www.praekelt.org/covid-19-response-in-sa)

R2K, "Fighting misinformation and defending free expression during COVID-19 (2020) (accessible at https://www.r2k.org.za/2020/04/23/covid19/)

R2K, "COVID-19 Surveillance Info Sheet" (2020) (accessible at https://www.r2k.org.za/2020/04/14/covid-19-surveillance-infosheet/)

Razzano, "Digital Hegemonies for COVID-19" (2020) (accessible at https://globaldatajustice.org/covid-19/digital-hegemonies-south-africa)

Reddy, "Privacy in the pandemic: The (mostly) untold story of digital contact tracing in SA" (2020) (accessible at https://www.dailymaverick.co.za/article/2020-12-06-privacy-in-the-pandemic-the-mostly-untold-story-of-digital-contact-tracing-in-sa/)

Research ICT Africa, "Despite reduction in mobile data tariffs, data still expensive in South Africa: Policy brief 2" (2020) (accessible at https://researchictafrica.net/publication/despite-reduction-in-mobile-data-tariffs-data-is-still-expensive-in-south-africa/)

Research ICT Africa, "Has South Africa's COVID Alert contact tracing app been zero-rated?" (2020) (accessible at https://researchictafrica.net/2020/09/25/has-south-africas-covid-alert-app-been-zero-rated/)

Right2Know Campaign (R2K) and Privacy International (PI), "State of Privacy in South Africa" (2019) (accessible at https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa#dataprotection)

Singh and Power, "New digital regulations mean the state can track you – no questions asked" (2020) (accessible at https://mg.co.za/article/2020-03-31-new-digital-regulations-mean-the-state-can-track-you-no-questions-asked/)

Statista, "Number of smartphone users in South Africa from 2014 to 2023" (2020) (accessible at https://www.statista.com/statistics/488376/forecast-of-smartphone-users-in-south-africa/#:~:text=Today%20about%2020%20to%2022,and%20on%20the%20continent%20overall)

Statistics South Africa, "Inequality Trends in South Africa: A multidimensional diagnostic of inequality" (2019) (accessible at http://www.statssa.gov.za/publications/Report-03-10-19/Report-03-10-192017.pdf)

Statistics South Africa, "General Household Survey" (2018) (accessible at http://www.statssa.gov.za/publications/P0318/P03182018.pdf)

Statistics South Africa, "Quarterly Labour Force Survey" (2020) (accessible at http://www.statssa.gov.za/?p=13652)

Transparency International, "In South Africa, COVID-19 has exposed greed and spurred long-needed action against corruption" (2020) (accessible at https://www.transparency.org/en/blog/in-south-africa-covid-19-has-exposed-greed-and-spurred-long-needed-action-against-corruption#)

World Bank, "Population, total – South Africa" (2019) (accessible at https://data.worldbank.org/indicator/SP.POP.TOTL?locations=ZA)

Speeches

President Cyril Ramaphosa, Developments in Coronavirus Covid-19 response (December 3, 2020) (accessible at https://www.gov.za/speeches/president-cyril-ramaphosa-developments-coronavirus-covid-19-response-3-dec-2020-0000)

President Cyril Ramaphosa, Extension of Coronavirus COVID-19 lockdown to the end of April (April 9, 2020) (accessible at https://www.gov.za/speeches/president-cyril-ramaphosa-extension-coronavirus-covid-19-lockdown-end-april-9-apr-2020-0000)

President Cyril Ramaphosa, Address by President Cyril Ramaphosa on South Africa's response to the coronavirus pandemic (June 17, 2020) (accessible at http://www.dirco.gov.za/docs/speeches/2020/cram0617.pdf)

News articles

Afriforum, "Afriforum wins case regarding COVID-19 Quarantine Camp" (May 6, 2020) (accessible at https://afriforum.co.za/en/afriforum-welcomes-judgement-on-covid-19-quarantine-camp/)

Arndt et al., "Impact of Covid-19 on the South African economy" (2020) (accessible at https://sa-tied.wider.unu.edu/sites/default/files/pdf/SA-TIED-WP-111.pdf)

Bhana, "Should I download the new contact tracing app?" (2020) (accessible at https://www.explain.co.za/2020/09/15/explainer-should-i-download-the-new-contact-tracing-app/)

Bloomberg, "Nigeria Tops South Africa as the Continent's Biggest Economy" (2020) (accessible at https://www.bloomberg.com/news/articles/2020-03-03/nigeria-now-tops-south-africa-as-the-continent-s-biggest-economy)

Business Insider, "More than half a million South Africans have now downloaded the Covid-19 tracing app" (22 September 2020) (accessible at https://www.businessinsider.co.za/half-a-million-south-africans-download-the-covid-tracing-app-2020-9).

Carlitz and Makhuru, "Life under lockdown: Illustrating trade-offs in South Africa's response to COVID-19" (2021) (accessible at https://www.sciencedirect.com/science/article/abs/pii/S0305750X20302953)

Fitch Ratings, "Fitch Downgrades South Africa to 'BB-'; Outlook Negative" (2020) (accessible at https://www.fitchratings.com/research/sovereigns/fitch-downgrades-south-africa-to-bb-outlook-negative-20-11-2020)

Georg, "Covid-19 contact tracing via chatbot? Rather consult a psychic" (July 30, 2020) (accessible at https://www.dailymaverick.co.za/opinionista/2020-07-30-covid-19-contact tracing-via-chatbot-rather-consult-a-psychic/)

Himbara, "South Africa: A sophisticated failing state" (2020) (accessible at https://www.theafricareport.com/35378/south-africa-a-sophisticated-failing-state/)

Hunter and Thakur, "Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but …" (2020) (accessible at https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but/)

Human Rights Watch, "South Africa: Widespread Xenophobic Violence" (September 17, 2020) (accessible at https://www.hrw.org/news/2020/09/17/south-africa-widespread-xenophobic-violence).

Information Regulator, "Information Regulator SA Provides Legal Analysis on Whatsapp Privacy Policy" (2021) (accessible at https://www.justice.gov.za/inforeg/docs/ms-20210303-Whatsapp.pdf)

Krige, "CoviID: new app to avoid future lockdowns" (2020) (accessible at https://www.news.uct.ac.za/article/-2020-03-27-coviid-new-app-to-avoid-future-lockdowns)

Makinana, "Collins Khosa murder: Military Ombud finds that soldiers acted improperly" (August 19, 2020) (accessible at https://www.timeslive.co.za/politics/2020-08-19-collins-khosa-murder-military-ombud-finds-that-soldiers-acted-improperly/)

McKane, "This graph shows how South African WhatsApp users are flocking to Telegram" (January 13, 2021) (accessible at https://mybroadband.co.za/news/it-services/382300-this-graph-shows-how-south-african-whatsapp-users-are-flocking-to-telegram.html).

McKinley, "New Terrains of Privacy in South Africa", Right2Know Campaign (2016) (accessible at https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf)

Medical Brief, "SA's heritage of community workers critical to stemming COVID-19 tide" (2020) (accessible at https://www.medicalbrief.co.za/archives/sas-heritage-of-community-workers-critical-to-stemming-covid-19-tide/)

Meyer, "Xenophobic #PutSouthAfricansFirst accounts 'fuelling social discord' online'" (September 9, 2020) (accessible at https://www.thesouthafrican.com/news/xenophobic-twitter-accounts-uct-bots-Wednesday-9-september/)

Mkhize, "Health Department launches COVID service portal" (2020) (accessible at https://sacoronavirus.co.za/2020/07/17/health-department-launches-covid-service-portal/)

Msomi, "Department of Health releases SA's first TB prevalence survey" (February 5, 2021) (accessible at https://www.news24.com/health24/medical/tuberculosis/news/department-of-health-releases-sas-first-tb-prevalence-survey-20210205)

Naude and Cameron, "Failing to Pull Together: South Africa's Troubles Response to COVID-19" (2020) (accessible at http://ftp.iza.org/dp13649.pdf)

NDOH, "COVID Alert SA app – data protection & privacy policy" (2020) (accessible at https://sacoronavirus.co.za/covidalert/privacy-policy/)

News24, "Taking on moron-a-virus: UCT launches a 6-month project to combat spread of COVID-19 fake news" (2020) (accessible at https://www.news24.com/news24/SouthAfrica/News/taking-on-moron-a-virus-uct-launches-6-month-project-to-combat-spread-of-covid-19-fake-news-20200506)

News24, "Don't clamp down on freedom of expression through criminalising spread of COVID-19 misinformation – legal officer" (2021) (accessible at https://www.news24.com/news24/southafrica/news/dont-clamp-down-on-freedom-of-expression-through-criminalising-spread-of-covid-19-misinformation-legal-officer-20210129)

News24, "Explainer: What is COVID-19 contact tracing and how does it work? We ask an expert" (2020) (accessible at https://www.news24.com/news24/southafrica/news/explainer-what-is-covid-19-contact-tracing-and-how-does-it-work-we-ask-an-expert-20200403)

Nkosi, "Government dragged to court for extending lockdown" (November, 18 2021) (accessible at https://www.iol.co.za/the-star/news/government-dragged-to-court-for-extending-lockdown-d952e4a1-6ebe-4cbf-a236-1b8815b6e812)

Nortier, "COVID Alert SA app: The fine balance between public health, privacy and the power of the people" (October 13, 2020) (accessible at https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/)

Nzimande, "Minister Blade Nzimande: Higher Education and Training response to Coronavirus Covid-19 epidemic lockdown level 1" (2020) (accessible at https://www.gov.za/speeches/education-sector-response-covid-19-epidemic-lockdown-30-sep-2020-0000)

PoliticsWeb, "Govt ramps us fake news monitoring – Jackson Mthembu" (2020) (accessible at https://www.politicsweb.co.za/politics/govt-ramps-up-fake-news-monitoring--jackson-mthemb)

Rickard, "Collins Khosa judgment: A win for all of South Africa against brutality by security forces" (May 18, 2020) (accessible at https://www.dailymaverick.co.za/article/2020-05-18-collins-khosa-judgment-a-win-for-all-of-south-africa-against-brutality-by-security-forces/)

SA News, "Register for HealthCheck before entering campuses" (June 10, 2020) South African Government News Agency (accessible at https://www.sanews.gov.za/south-africa/register-healthcheck-entering-campuses).

SAPS, "Media Statement South African Police Service Office of the Provincial Commissioner Eastern Cape" (2020) (accessible at https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=28349)

SAPS, "Media Statement South African Police Service Office of the Provincial Commissioner Gauteng" (2020) (accessible at https://www.saps.gov.za/newsroom/selnewsdetails.php?nid=28467)

Seleka, "JSC refers Mogoeng's 'devil' vaccine prayer remarks to judicial conduct committee" (January 13, 2021) (accessible at https://www.news24.com/news24/southafrica/news/jsc-refers-mogoeng-devil-vaccine-prayer-remarks-to-judicial-conduct-committee-20210113)

Shoba, "Government action plan fails to curb xenophobic violence in SA" (September 17, 2020) (accessible at https://www.dailymaverick.co.za/article/2020-09-17-government-action-plan-fails-to-curb-xenophobic-violence-in-sa/)

Simelane, "Covid-19 and the call for solidarity: Challenges for informal settlements" (April 12, 2020) (accessible at https://mg.co.za/article/2020-04-12-covid-19-and-the-call-for-solidarity-challenges-for-informal-settlements/)

Smit, "Police treat sex workers like they are 'nothing'" (June 10, 2020) (accessible at https://mg.co.za/news/2020-06-10-police-treat-sex-workers-like-they-are-nothing/)

Smith, "A threat to Democracy: COVID-19 has exposed how big fake news in SA is – experts" (January 29, 2021) (accessible at https://ewn.co.za/2021/01/29/a-threat-to-democracy-covid-19-has-exposed-how-big-fake-news-in-sa-is-experts)

Soer, "Sex, Drugs and COVID-19" (July 3, 2020) (accessible at https://www.csagup.org/2020/07/03/sex-drugs-and-covid-19/)

Sonjica, '"The app will give you stress,' says user. But Covid-19 alert app's effectiveness depends on you, say experts" (January 25, 2021) *Sunday Times* (accessible at https://www.timeslive.co.za/sunday-times-daily/news/2021-01-25-the-app-will-give-you-stress-says-user-but-covid-19-alert-apps-effectiveness-depends-on-you-say-experts/)

Travelstart, "International Travel Information" (2020) (accessible at https://www.travelstart.co.za/lp/international-travel-information)

Trippe, "Pandemic policing: South Africa's most vulnerable face a sharp increase in police-related brutality" (June 24, 2020) (accessible at https://www.atlanticcouncil.org/blogs/africasource/pandemic-policing-south-africas-most-vulnerable-face-a-sharp-increase-in-police-related-brutality/)

Turn, "SA National Department of Health launches HealthCheck, a COVID-19 digital health-assessment tool" (2020) (accessible at https://www.turn.io/news/ndoh-covid-connect)

University of Pretoria, "Message to the UP Community regarding HealthCheck App" (2020) (accessible at https://www.up.ac.za/coronavirus-updates/article/2900121/healthcheck-app-message-to-the-up-community)

Voigt, "COVID-19: The trail and error of digital contact tracing in SA" (July 28, 2021) (accessible at https://www.spotlightnsp.co.za/2020/07/28/covid-19-the-trial-and-error-of-digital-contact-tracing-in-sa/)

Websites

National Department of Health, "SA Coronavirus: Online Resources & News Portal" (accessible at https://sacoronavirus.co.za/)

U.S. Embassy & Consulates in South Africa, "COVID-19 Information" (March 2021) (accessible at https://za.usembassy.gov/covid-19-information-2/)

Technical Report

"Report on the privacy risks of COVID-19 software" (2020)

question convention

altadvisory

.africa